

RULE 6A-1.0955 AMENDMENT

The School Board of Citrus County, Florida

THIS RULE 6A-1.0955 AMENDMENT is made by and between The School Board of Citrus County, Florida, a political subdivision of the State of Florida (“**School Board**”) and Zoom Video Communications, Inc. (“**Provider**”), and is intended to modify the Terms of Service, Master Subscription Agreement, or any other agreement previously entered into by School Board and Provider with respect to Provider’s delivery of the contracted services (the “**Prior Agreement**”). School Board and Provider may also be referred to herein each as a “**Party**” and collectively as the “**Parties**”.

WHEREAS, School Board is responsible for operating and controlling all public K-12 schools located in Citrus County, Florida (collectively referred to herein as “**Citrus County Schools**”) and is the statutory contracting agent for Citrus County Schools.

WHEREAS, Rule 6A-1.0955 of the Florida Administrative Code was promulgated by the Florida Department of Education with an effective date of November 22, 2022 (the “**Rule**”).

WHEREAS, the Rule requires certain additional terms and conditions be incorporated into all existing and future agreements that involve or may involve any disclosure or use of student personally identifiable information (“**PII**”).

WHEREAS, School Board and Provider believe the Prior Agreement may be subject to the Rule.

NOW, THEREFORE, in consideration of the premises and of the mutual covenants contained herein and to bring the Prior Agreement into compliance with the Rule, the Parties hereby agree to amend and modify the Prior Agreement as follows:

1. The above Recitals are incorporated herein by reference.
2. Attachment “A” below, including all exhibits attached thereto, is fully incorporated into and made a part of the Prior Agreement.
3. Provider shall promptly notify School Board in writing concerning needed updates to Attachment “A”, Exhibit “B” (Schedule of Data) due to any material changes that impact the disclosure or use of PII (“**Needed Changes**”), after which the Parties shall modify said Exhibit “B” accordingly. Failure by Provider to notify School Board of any Needed Changes shall constitute default and a material breach of the Prior Agreement and provide School Board the option, but not the obligation, to immediately terminate the Prior Agreement without penalty. For clarification, any optional features that Provider may offer for the SDPA Services which LEA may choose to add to the SDPA Services do not constitute Needed Changes.
4. The effective date of this Amendment shall be the date of full execution by the Parties.
5. This Amendment may be executed in counterparts, whether signed physically or electronically, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

ATTACHMENT A
STUDENT DATA PRIVACY AGREEMENT

THIS STUDENT DATA PRIVACY AGREEMENT (“**SDPA**”), as developed by the Student Data Privacy Consortium (“**SDPC**”) and modified by the local education agency identified herein, is entered into on the date of full execution (the “**Effective Date**”) by and between The School Board of Citrus County, Florida, a political subdivision of the State of Florida and designated local education agency for purposes of this SDPA (“**LEA**”) and Zoom Video Communications, Inc. (“**Provider**”). LEA and Provider may also be referred to herein each as a “**Party**” and collectively as the “**Parties**”.

WHEREAS, Provider is obligated under that certain Master Subscription Agreement or terms of service by and between Provider and LEA (the “**Service Agreement**”), to provide certain educational or digital services to LEA.

WHEREAS, 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).

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

NOW THEREFORE, in consideration of the mutual promises, covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which is acknowledged by the Parties, LEA and Provider hereby agree as follows:

1. The SDPC Standard Clauses, as attached hereto (the “**Standard Clauses**”), are fully incorporated into and made a part of this SDPA.
2. The following, only if checked, shall be fully incorporated into and made a part of this SDPA (collectively referred to herein as the “**Special Provisions**”):
 - Supplemental State Terms as set forth in **Exhibit “G”** attached to the Standard Clauses.
 - Additional terms or modifications set forth in **Exhibit “H”** attached to the Standard Clauses.
 - General Offer of Privacy Terms as set forth in **Exhibit “E”** attached to the Standard Clauses.
3. In the event of a conflict between the Standard Clauses and the Special Provisions, the terms of the Special Provisions will control. In the event there is conflict between the terms of the

SDPA and any other writing, including, but not limited to the Service Agreement and any terms of service or privacy policy of Provider, the terms of this SDPA shall control with respect to the subject matter of protecting Student Data.

4. A description of the services to be provided and the categories of student data that may be provided by LEA to Provider, and other information specific to this SDPA are contained in the Standard Clauses.
5. A description of the services to be provided by Provider to LEA pursuant to this SDPA are contained in **Exhibit "A"** to the Standard Clauses (the "**SDPA Services**").
6. The term of this SDPA shall end upon the termination or expiration of the Service Agreement.
7. 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:

LEA-designated Representative:

Name: Kathy Androski_____

Title: Director of Educational Technology_____

Address: 3741 W. Educational Path, Lecanto, FL 34461__

Phone: (352) 746-3437_____

Email: AndroskiK@citruschools.org_____

Provider-designated Representative:

Name: Deborah Fay_____

Title: Data Protection Officer_____

Address: 55 Almaden Blvd, San Jose, CA, 95113, Suite 600


Phone: +353 1 582 7141_____

Email: deborah.fay@zoom.us, with a copy to legal@zoom.us

IN WITNESS WHEREOF, LEA and Provider have executed this SDPA on the dates set forth below.

The School Board of Citrus County, Florida



By: 
Douglas A. Dodd, Chairman

Date: 10/10/2023

Zoom Video Communications, Inc.

By: 

Name: Deborah Fay

Date: Oct 2, 2023



SDPC STANDARD CLAUSES

Version 1.0

Article I. ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of SDPA.** The purpose of this SDPA 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 pertaining to Student Data, all as may be amended from time to time. In performing the SDPA Services, Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by LEA. Provider shall be under the direct control and supervision of LEA, with respect to its use of Student Data.
2. **Student Data to Be Provided.** In order to perform the SDPA Services, LEA shall provide to Provider certain Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **SDPA Definitions.** The definition of terms used in this SDPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this SDPA shall prevail over terms used in any other writing pertaining to the subject matter herein, including, but not limited to the Service Agreement and any terms of service or privacy policies of Provider.

Article II. ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of LEA. Provider further acknowledges and agrees that all copies of such Student Data transmitted to Provider, including any modifications or additions or any portion thereof (excluding De-Identified Data) from LEA or its authorized designee, are subject to the provisions of this SDPA in the same manner as the original Student Data. The Parties agree that as between them, all rights in and to Student Data, including all intellectual property rights therein, shall remain the exclusive property of LEA. For the purposes of FERPA, Provider shall be considered a School Official, under the control and direction of LEA as it pertains to the use of Student Data.
2. **Parent Access.** To the extent required by law, LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and Student Data and correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. To the extent the Provider has access to the data Provider shall respond in a reasonably timely manner (but no later than forty-five (45) days from the date of the request or the time frame required under state law for LEA to respond to a parent or student, whichever is sooner) to LEA’s request for Student Data in a student’s records held by Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts Provider to review any of the Student Data accessed pursuant to the Services, Provider shall refer the parent or individual to 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 Provider, then Provider shall, at the request of LEA, transfer, or provide a mechanism for 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 (each a “Requesting Party”) contact Provider with a request for Student Data held by Provider pursuant to the SDPA Services, Provider shall notify LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform LEA of the request, and any such notification to LEA will be in accordance with Provider’s government requests guide. LEA is on notice of and has reviewed Provider’s government requests guide located at <https://explore.zoom.us/cn/trust/government-requests-guide/>, and LEA acknowledges that this SDPA does not restrict Provider’s right to modify the government requests guide from time to time.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for Provider in order for Provider to provide the Services (as defined in the Service Agreement), whereby each Subprocessor agrees to protect Student Data in a manner no less stringent than the terms of this SDPA. LEA is on notice of Provider’s Subprocessors listed [here](#), and LEA acknowledges that this SDPA does not restrict Provider’s right to modify its Subprocessors from time to time.

Article III. **ARTICLE III: DUTIES OF LEA**

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the SDPA 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 LEA has a policy of disclosing Education Records or Student Data under FERPA (34 CFR § 99.31(a)(1)), then 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 protect Student Data by implementing administrative, physical, and technical safeguards, including those specifically designed to secure usernames, passwords, and any other means of gaining access to the SDPA Services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly and in all cases within seventy-two (72) hours of any known unauthorized access to Student Data or the SDPA Services. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.
5. **Use of Services and Consents.** LEA shall use the SDPA Services solely for educational purposes when using it with children under 13. LEA consents to Provider’s collection practices described in its Children’s Educational Privacy Statement located [here](#). LEA verifies that it is authorized to provide consent on behalf of its organization. LEA shall obtain any necessary parent or guardian consent for any third-party apps that LEA chooses to allow children to use in connection with the SDPA Services. LEA is on notice of Provider’s Privacy Statement [here](#) and the aforementioned

Children's Educational Privacy Statement, each of which LEA acknowledges and is aware of and consents to Provider's right to modify these policies from time to time.

Article IV. **ARTICLE IV: DUTIES OF PROVIDER**

1. **Privacy Compliance.** Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security applicable to Provider in its performance of the SDPA Services, 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 to deliver the SDPA Services outlined in **Exhibit "A"**, or stated in the Service Agreement, or otherwise authorized under the statutes referred herein.
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 SDPA with respect to the Student Data shared as a result of Provider's delivery of the SDPA Services to LEA. Provider agrees to require and maintain an employee nondisclosure 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 non-public information or personally identifiable information contained in the Student Data other than as directed or permitted by LEA, applicable law, or this SDPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified Data, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing any work on behalf of Provider pursuant to this SDPA. Provider shall not sell Student Data to any third party.
5. **De-Identified Data.** Provider agrees not to attempt to re-identify De-Identified Data. De-Identified Data may be used by Provider for those purposes allowed under FERPA and the following purposes: (1) assisting LEA or other governmental agencies in conducting research and other studies; and (2) research and development of Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the SDPA Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this SDPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer De-Identified 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 LEA who has provided prior written consent for such transfer. Prior to publishing any document that names LEA explicitly or indirectly, Provider shall obtain LEA's written approval of the manner in which De-Identified Data is presented.
6. **Disposition of Data.** Upon written request from LEA, Provider shall provide a mechanism for LEA to transfer Student Data obtained under the Service Agreement and held by Provider. If there is a written request from LEA, Provider will delete Student Data 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 SDPA and the Service Agreement, if no written request from LEA is received, Provider shall thereafter remove LEA access, dispose of all Student Data or

both in accordance with Provider's practices, procedures, and data deletion policies. 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 Article II, Subsection 3. LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If LEA and Provider employ **Exhibit "D"**, then 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 SDPA Services 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 SDPA and its accompanying exhibits.

Article V. **ARTICLE V: DATA PROVISIONS**

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States when US servers are selected by the LEA admin in the Provider's admin console. Upon request of LEA, Provider will provide a list of the locations where Student Data is stored. LEA acknowledges that certain Student Data may be disclosed or accessed outside the United States during a technical support engagement initiated by LEA.
2. **Audits.** No more than once a year, or following unauthorized access of Student Data, upon receipt of a written request from LEA with at least ten (10) business days' written notice and upon the execution of an appropriate confidentiality agreement, Provider shall allow LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of the SDPA Services to LEA. Provider will cooperate reasonably with LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of Provider or delivery of SDPA Services to students or LEA. The Provider will share its customer facing third party audit reports applicable to LEA upon written request from LEA on an annual basis. Provider may require additional terms of confidentiality as a condition to receipt of Provider's sensitive security-related information.
3. **Data Security.** Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. Provider and LEA shall adhere to any applicable law relating to data security. Provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Provider shall designate an employee to serve as LEA's primary contact regarding any data security concerns or questions.
4. **Data Breach.** In the event of a confirmed unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by Provider, Provider shall notify LEA in writing within seventy-two (72) hours of confirmation of the incident unless the timing of such notification would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a

reasonable time after the incident. Provider shall follow the following process:

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by 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 Student Data 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. 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
 - iv. 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 applicable federal and state requirements with respect to a data breach related to the Student Data.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and applicable 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 SDPA Services, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

Article VI. **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 Subscribing LEA who signs the acceptance on said Exhibit E. 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 SDPA, they may do so by mutual written consent. Either party may terminate this SDPA and the Service Agreement if the other party materially breaches any terms of this SDPA and fails to cure the breach within thirty

(30) days or another reasonable time agreed to by the parties in a duly signed writing.

2. **Effect of Termination and Survival.** If the Service Agreement and this SDPA are terminated, then Provider shall return or destroy all of LEA's Student Data in accordance with Provider's data deletion and destruction policies. Irrespective of termination of the Service Agreement and this SDPA, the obligations of Provider under this SDPA will continue until Provider has returned or destroyed all of the LEA's Student Data.
3. **Reserved.**
4. **Entire Agreement.** This SDPA constitutes 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 SDPA may be amended and the observance of any provision of this SDPA 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 SDPA 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 SDPA, 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, then it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this SDPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS SDPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF FLORIDA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS IN THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SDPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This SDPA is and shall be binding upon the respective successors and assigns of 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 Provider sells, merges, or otherwise disposes of its business or assets to a successor during the term of this SDPA, Provider shall provide written notice to LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. LEA has the authority to terminate the SDPA if the LEA is prohibited from: (a) performing under this SDPA pursuant to a decision by a court or regulatory body of competent jurisdiction; or (b) contracting with the successor entity pursuant to applicable law. If LEA exercises its right to terminate this SDPA pursuant to

sections (a) or (b) in the preceding sentence, then LEA must exercise such right within sixty (60) days of the event, otherwise the right to terminate will be automatically waived.

8. **Authority.** Each party represents that it is authorized to enter into this DPA and that the signatory is duly authorized to sign this DPA. .
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.

EXHIBIT A
DESCRIPTION OF SERVICES

Please describe the functionality of the product and include if the application is a subscription or free online service. Also, include if the data is stored exclusively in the United States. If not, then list the countries in which data is stored.

<https://explore.zoom.us/en/services-description/>

Student Data is stored in the United States. LEA acknowledges that certain Student Data may be disclosed or accessed outside the United States during a technical support engagement initiated by LEA.

EXHIBIT B
SCHEDULE OF DATA – To be completed by the vendor

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X
	Other application technology meta data-Please specify: device type and features (such as camera version), technical product usage, settings (such as audio, video, screen sharing settings)	X
Application Use Statistics	Meta data on user interaction with application	X
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)	X
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)	

Category of Data	Elements	Check if Used by Your System
	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 (optional and only applicable if provided)	X
	Teacher names (optional and only applicable if provided)	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	

Category of Data	Elements	Check if Used by Your System
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
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 (optional and only applicable if provided)	X
Student work	Student generated content; writing, pictures, etc. (optional and only applicable if provided)	X

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	
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 data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application: profile picture if provided/optional	X

General	The categories of information in the privacy information, general information as provided in Provider's Privacy Statement (found here) and Provider's Children's Educational Privacy Statement (found here). This does not incorporate the terms from these documents into the SDPA.	X
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 or an individual's device.

Education Records: Education Records are defined by applicable law and, if not defined, 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 or Student Data.

Operator: means an Operator as defined by applicable law and, if not defined, an 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 this SDPA in its entirety with Provider.

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 SDPA and pursuant to 34 CFR § 99.31(b), a School Official is a provider that: (1) Performs an institutional service or function for which the agency or institution would otherwise use its own employees; (2) Is via this SDPA 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.

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, except to the extent expressly excluded under the definition of Metadata above. 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 SDPA, 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 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 SDPA, the term “Subprocessor” means an entity that is not LEA or Provider, engaged by Provider to process Student Data on behalf of the LEA per the LEA's instructions under the terms of this SDPA or the Service Agreement. Authorized Subprocessors may include Provider’s affiliates but shall exclude Provider employees, contractors and consultants.

Subscribing LEA: means an LEA who accepts Provider’s General Offer of Privacy Terms and is under a service agreement with Provider.

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.

EXHIBIT D
DIRECTIVE FOR DISPOSITION OF DATA

LEA hereby directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider as follows:

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 Personally Identifiable Information.

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.

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT E
GENERAL OFFER OF PRIVACY TERMS

OFFER OF TERMS:

Provider offers the same privacy protections found in this SDPA between it and The School Board of Citrus County, Florida (“**Originating LEA**”) which is dated [Insert Date], to any other local education agency (“**Subscribing LEA**”) who accepts this General Offer of Privacy Terms (“**General Offer**”) through its signature below. This General Offer shall extend only to privacy protections set forth in this SDPA, and Provider’s signature below shall not bind Provider to any other terms, such as price, term, or schedule of services, or to any other provision not addressed in this SDPA. Any changes to this Exhibit E template are null and void, however, Provider and the Subscribing LEA may agree to change the data provided by Subscribing LEA to Provider to suit the unique needs of the Subscribing LEA. Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the Service Agreement; or (3) at the end of the term set forth in this SDPA. To indicate Subscribing LEA’s acceptance, the Subscribing LEA must send the signed **Exhibit “E”** to Provider at the following email address:

PROVIDER NAME: Zoom Video Communications, Inc.

BY: _____
Date: Oct 2, 2023
Printed Name: Deborah Fay
Title/Position: Deputy General Counsel

ACCEPTANCE BY SUBSCRIBING LEA:

Subscribing LEA, by signing a separate service agreement with Provider, and by its signature below, hereby accepts this General Offer of Privacy Terms. Subscribing LEA and Provider shall therefore be bound by the same terms of this SDPA for the term of this SDPA between The School Board of Citrus County, Florida and Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER AND PROVIDER MUST PROVIDE A CONFIRMATION OF RECEIPT IN ORDER FOR THIS GENERAL OFFER TO TAKE EFFECT. ****

SUBSCRIBING LEA NAME: The School Board of Citrus County Florida
BY: _____
Date: 10/10/2023
Printed Name: Douglas A. Dodd
Title/Position: Chairman

LEA'S DESIGNATED REPRESENTATIVE:

Name: Kathy Androski_____

Title: Director of Educational Technology_____

Address: 3741 W. Educational Path, Lecanto, FL 34461_____

Telephone Number: (353) 746-3437_____

Email: AndroskiK@citruschools.org_____

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)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located [here](#)

EXHIBIT G
SUPPLEMENTAL SDPC STATE TERMS FOR FLORIDA

Version _____

None

EXHIBIT H
ADDITIONAL TERMS OR MODIFICATIONS

None

Children's Educational Privacy Statement

Last updated: September 2021

This Children's Educational Privacy Statement ("Statement") describes the personal data we collect, use or disclose from students under the age of 18 when they receive educational services from schools and other organizations who are using Zoom Video Communication, Inc.'s ("Zoom") meetings, webinars, or messaging platform ("Zoom Products") to provide educational services to children. This Statement supplements Zoom's Privacy Statement and applies only if the account settings selected by a school or organization confirm that it provides educational services to children under 18.

What Personal Data Does Zoom Collect from Students?

Personal data is any information from or about an identified or identifiable person, including information that Zoom can associate with an individual person. We may collect, or process on behalf of schools or other organizations providing educational services, the following categories of personal data when a student uses or interacts with Zoom Products to receive educational services, such as when they join their classroom or meet with their teacher on Zoom:

- **Profile and Participant Information:** Name, profile picture, contact information, and any other information a school or educational organization allows students to add to their profile or to add when registering for meetings, recordings or webinars hosted on the school or organization's account.
- **Contacts and Calendar Information:** Contact lists the school or educational service adds or allows students to use on their account (such as names and email addresses for other students in the school), as well as calendar information added to the account (such as a class schedule or upcoming school events).
- **Settings:** Preferences and settings students set when using an educational account, such as microphone, audio and video settings, and screen sharing settings.
- **Device Information:** Information about the computers, phones, and other devices students use when joining meetings or webinars or sending messages using Zoom Products, including device features (like microphone or camera versions and IDs), IP address (which may be used to infer general location at a city or country level) and WiFi information.
- **Meeting, Webinar, and Messaging Content:** If the school or educational organization chooses to record meetings or webinars to Zoom Cloud, Zoom will store these recordings on behalf of the school or organization. The recordings may contain a student's voice and image, messages, Q&A, or other content (such as a presentation or whiteboard) shared by a student during a meeting or webinar. Zoom employees do not access this content unless the school or educational service directs us to do so, or as required for legal, security, or safety reasons.
- **Product Usage:** Information about how students and their devices interact with Zoom Products, such as when they join and leave a meeting, whether they send messages and with whom they message, mouse movements, clicks, keystrokes, or actions (such as mute/unmute or video on/off), and other inputs that help Zoom understand feature usage, improve product design, and suggest features.

How Do We Use Student Personal Data?

Zoom uses personal data collected from students to conduct the following activities:

- **Provide Educational Products and Services:** To provide products, features and services for schools and other organizations to use when providing educational services to children, including to customize the product and safety features and settings for a school environment. This may also include using personal data for customer support, which may include accessing audio, video, files, and messages, at the direction of the school or organization.
- **Product Research and Development:** To develop, test, and improve Zoom Products that are used in educational settings.
- **Authentication, Integrity, Security, and Safety:** To authenticate accounts and activity, detect, investigate, and prevent malicious conduct or unsafe experiences, address security threats, protect school and public safety, and secure Zoom Products.
- **Legal Reasons:** To comply with applicable law or respond to valid legal process, including from law enforcement or government agencies, to investigate or participate in civil discovery, litigation, or other adversarial legal proceedings, and to enforce or investigate potential violations of our Terms of Service or policies.

Zoom uses advanced tools to automatically scan content such as virtual backgrounds, profile images, and files uploaded or exchanged through chat, for the purpose of detecting and preventing violations of our terms or policies and illegal or other harmful activity, and its employees may investigate such content where required for legal, safety, or security reasons.

How Do We Share Student Personal Data?

Zoom does not disclose student's data to third parties, except for:

- service providers who help us provide Zoom Products and technical infrastructure;
- where required for legal, security, or safety reasons;
- or to other Zoom affiliates (such as Zoom Voice Communications, Inc., which provides Zoom Phone) to enable additional products and features for use by schools and educational organizations.

What Student Information Do Schools See and Share on Zoom Products?

Depending on their policies, settings and how they use Zoom Products to provide educational services, the school or organization providing educational services may be able to see or to share the following personal data from students who join meetings or webinars on their account. The school or other organization's use and disclosure of student information is subject to the school or educational organization's policies, not Zoom's. Zoom does not enable children to make personal information publicly available through the use of Zoom Products.

- **Student Usage and Content:** Depending on their settings, the school or other organization providing educational services – and the people they designate – can access (i) information about how students and their devices interact with the school or educational organization's account; (ii) information about the participants who joined classrooms or meetings on their account (including participant name, display name, email address and participant ID); (iii) the content of recordings hosted on their account, as well as a transcript of audio, if enabled; and (iv) information provided in response to polls, Q&A or other content shared during classrooms, webinars and meetings on their account.
- **Teachers, Hosts and Participants:** Teachers, hosts and other participants in a classroom or meeting may be able to see students' email, display name, and profile picture, as well as content and information shared by students during

a meeting and webinar. Depending on settings implemented by the school or educational organization, teachers, hosts and participants also may be able to record or save classroom or meeting content, audio transcripts, messages sent to Everyone or to them directly, and files, whiteboards, or other information shared during a classroom or educational meeting.

- **Third-Party App:** Schools or educational organizations may choose to install third-party apps to add features or educational services to their use of Zoom Products, including apps that may receive access to personal information about students and other users on their account. Zoom does not pre-install any apps on educational accounts, and apps will not be able to access personal information from students receiving educational services on Zoom Products unless the school or educational organization chooses to approve a specific app. Personal information shared by schools and educational organizations with third-party apps is subject to the school or organization's policies and the app developers' terms and privacy policies, not Zoom's.

In the United States, before choosing to install third party-apps that may be used by children under the age of 13, schools or educational organizations must obtain parent or guardian consent to the third-party app's data practices. By installing any third-party app, these schools or other educational organizations agree to obtain such parent or guardian consent and must consent themselves to the disclosure of students' personal information to the third-party app when installing the app.

How to Review and Delete Student Information

A school or other educational organization may review and delete a student's information, if in compliance with any applicable law, from their administrator dashboard. If you are a parent or student, please contact your school or other educational organization to access any personal information, limit a student's access to Zoom Products features or services, or delete personal information or the student's entire profile. A school or other educational organization may also take steps to prevent a student from receiving educational services through the use of Zoom Products on its account in the future, such as by deleting the student's profile from the school or other educational organization's account and limiting the student's access to use of Zoom.

How to Contact Us

If you are a parent or guardian:

- Contact your school administrator if you have questions regarding:
 - the school's management of its Zoom account
 - the school's use of your child's information
 - third-party apps approved by the school who may have access to your child's information
 - exercising your privacy rights with regards to education records
- Contact Zoom using the below contact information if you have questions regarding:
 - this Statement
 - Zoom's use of student's information

If you are an administrator for an organization providing educational services to students under 18 years of age, contact Zoom about the information in this Statement using the contact information below.

educationalprivacy@zoom.us

1-888-799-0182

Zoom Privacy Statement

Last updated: August 11, 2023

This Privacy Statement describes the personal data we collect and/or process (which may include collecting, organizing, structuring, storing, using, or disclosing) to provide products and services offered directly by Zoom Video Communications, Inc. ("Zoom"), including Zoom's websites, its meetings, webinars, and messaging platform, related collaborative features, and Zoom App Marketplace ("Zoom products and services" or "products and services"). Zoom products and services covered in this Privacy Statement do not include products or services developed by Zoom that are covered under a separate privacy policy (including those listed here).

California residents, please see our California Privacy Notice at Collection, and California & Other U.S. State Privacy Rights sections.

[What Personal Data Do We Receive?](#)

[How Do We Use Personal Data?](#)

[How Do We Share Personal Data?](#)

[Who Can See, Share, and Process My Personal Data When I Join Meetings and Use Other Zoom Products and Services?](#)

[Privacy Rights and Choices](#)

[Children](#)

[How to Contact Us](#)

[Retention](#)

[European Data Protection Specific Information](#)

[California & Other U.S. States Notice at Collection](#)

[California & Other U.S. State Privacy Rights](#)

[Changes to This Privacy Statement](#)

What Personal Data Do We Receive?

Personal data is any information from or about an identified or identifiable person, including information that Zoom can associate with an individual person. We may collect, or process on behalf of our customers, the following categories of personal data when you use or interact with Zoom products and services:

- **Account Information:** Information associated with an account that licenses Zoom products and services, which may include administrator name, contact information, account ID, billing and transaction information, and account plan information.
- **Profile and Participant Information:** Information associated with the Zoom profile of a user who uses Zoom products and services under a licensed account or that is provided by an unlicensed participant joining a meeting, which may include name, display name, picture, email address, phone number, job information, stated locale, user ID, or other information provided by the user and/or their account owner.
- **Contact Information:** Contact information added by accounts and/or their users to create contact lists on Zoom products and services, which may include contact information a user integrates from a third-party app, or provided by users to process referral invitations.
- **Settings:** Information associated with the preferences and settings on a Zoom account or user profile, which may include audio and video settings, recording file location, screen sharing settings, and other settings and configuration information.
- **Registration Information:** Information provided when registering for a Zoom meeting, webinar, Zoom Room, or recording, which may include name and contact information, responses to registration questions, and other registration information requested by the host.
- **Device Information:** Information about the computers, phones, and other devices used when interacting with Zoom products and services, which may include information about the speakers, microphone, camera, OS version, hard disk ID, PC name, MAC address, IP address (which may be used to infer general location at a city or country level), device attributes (like operating system version and battery level), WiFi information, and other device information (like Bluetooth signals).
- **Content and Context from Meetings, Webinars, Messaging, and Other Collaborative Features:** Content generated in meetings, webinars, or messages that are hosted on Zoom products and services ("Customer Content"), which may include audio, video, in-meeting messages, in-meeting and out-of-meeting whiteboards, chat messaging content, transcriptions, transcript edits and recommendations, written feedback, responses to polls and Q&A, and files, as well as related context, such as invitation details, meeting or chat name, or meeting agenda. Customer Content may contain your voice and image, depending on the account owner's settings, what you choose to share, your settings, and what you do on Zoom products and services. As referenced below, Zoom employees do not access or use Customer Content without the authorization of the hosting account owner, or as required for legal, safety, or security reasons.
- **Usage Information Regarding Meetings, Webinars, Messaging, Collaborative Features and the Website:** Information about how people and their devices interact with Zoom products and services, such as: when participants join and leave a meeting; whether participants sent messages and who they message with; performance data; mouse movements, clicks, keystrokes or actions (such as mute/unmute or video on/off), edits to transcript text, where authorized by the account owner and other inputs that help Zoom to understand feature usage, improve product design, and suggest features; which third-party apps are added to a meeting or other product or service and what information and actions the app is authorized to access and perform; use of third-party apps and the Zoom App Marketplace; features used (such as screen sharing, emojis, or filters); and other usage information and metrics. This also includes information about when and how people visit and interact with Zoom's websites, including what pages are accessed, interaction with website features

including Zoom's website's virtual chat feature, and whether or not the person signed up for a Zoom product or service.

- **Limited Information from Zoom Email and Calendar Services:** "Zoom Email" refers to Zoom's native email service and emails sent from Zoom's native email service. Zoom Email is designed to be end-to-end encrypted by Zoom by default for emails sent and received directly between active Zoom Email users. Support for end-to-end encryption requires Zoom Email users to have added a device to their Zoom Email account with the associated email address and to use a supported Zoom client. When an email is end-to-end encrypted, only the users, and, depending on their settings, account owners, or designated account administrators control the encryption key and therefore access to the email content, including body text, subject line, attachments and custom labels applied to messages by users in their inboxes. Emails sent to or received from non-Zoom Email users are encrypted after the email is sent or received from Zoom's servers, if the Zoom Email user chooses to send them with encryption. In all cases, Zoom does have access to email metadata used for basic email delivery—specifically, email addresses in the from, to, cc, and bcc fields, time, mimeType, and the number and size of attachments. From use of Zoom's native calendar service, Zoom receives information regarding meeting invitations, body text, sender and recipients, and other calendar information.
- **Content from Third-Party Integrations:** Users can access email and calendars from third-party services through their Zoom client, if they choose to integrate them. This information is not end-to-end encrypted by Zoom, but Zoom employees do not access the contents of third-party-service email or calendar entries, unless authorized to, or required for legal, safety, or security reasons. If account owners and/or their licensed end users integrate their third-party emails with products and services offered or powered by Zoom, such as business analytics tools like Zoom Revenue Accelerator Zoom may collect or process Customer Content and email information, including email content, headers and metadata, from such third-party services.
- **Communications with Zoom:** Information about, and contents of, your communications with Zoom, including relating to support questions, website virtual chats, your account, and other inquiries.
- **Information from Partners:** Zoom obtains information about account owners and their users from third-party companies, such as market data enrichment services, including information about an account owner's company size or industry, contact information, or activity of certain enterprise domains. Zoom may also obtain information from third-party advertising partners that deliver ads displayed on Zoom products and services, such as whether you clicked on an ad they showed you.

In certain jurisdictions, some of the personal data Zoom receives may be considered sensitive. Please see "California & Other U.S. State Privacy Rights" for more information.

How Do We Use Personal Data?

Zoom employees do not access or use Customer Content including meeting, webinar, messaging, or email content (specifically, audio, video, files, in-meeting whiteboards, messaging, or email contents), or any content generated or shared as part of other collaborative features (such as out-of-meeting whiteboards), unless authorized by the account owner hosting the Zoom product or service where the Customer Content was generated, or as required for legal, safety, or security reasons. **Zoom does not use any of your audio, video, chat, screen sharing, attachments or other communications-like Customer Content (such as poll results, whiteboard and reactions) to train Zoom's or third-party artificial intelligence models.**

As discussed below, and where technically feasible, Zoom uses personal data to conduct the following activities:

- **Provide Zoom Products and Services:** To provide and develop products and services to account owners, their licensed end users, and those they invite to join meetings and webinars hosted on

their accounts, including to customize Zoom products and services and recommendations for accounts or their users. Zoom also uses personal data to determine what products and services may be available in your location, and uses personal data, including contact information, to route invitations, messages, or Zoom Emails to recipients when users send or receive invitations, messages, or Zoom Emails using Zoom products and services. This may also include using personal data for customer support, which may include accessing audio, video, files, messages, and other content or context, at the direction of the account owner or their users. We also use personal data to manage our relationships and contracts with account owners and others, including billing, compliance with contractual obligations, facilitating payment to third-party developers in relation to purchases made through the Zoom App Marketplace, and related administration.

- **Advanced Audio and Video Features:** If you elect to turn on certain video features, if available in your area, such as filters, studio effects, avatars, and gestures, information about your movements or the positioning of your face or hands may be processed on your device to apply the selected features. Such data does not leave your device, is not retained, cannot be used to identify you, and is only used to generate the selected effects. If certain other features are enabled by the account owner hosting a Zoom product or service, such as transcription generation for recordings, Zoom may use technology that analyzes the meeting's audio recording to distinguish one speaker from another in order to create an accurate transcript. The audio analysis is not retained after the transcript is generated.
 - If you elect to turn on personalized audio isolation, software on your device will capture and analyze a clip of your audio from meetings you join to create an Audio Signature used to differentiate your voice from, and suppress background noise in, meetings you join. Zoom does not receive or retain the clip or Audio Signature, which stays on your device and is only used for noise suppression in meetings you join. You may delete the Audio Signature from your device through your Zoom app settings.
- **Intelligent Features:** If enabled by the account owner, Zoom provides intelligent features and products to its customers, their licensed end users and guests, such as Zoom AI Companion or other tools to recommend chat, email or other content. These tools may use artificial intelligence, machine learning, or other technology to process Customer Content solely to provide the intelligent features.
- **Product Research and Development:** If authorized by any applicable customer settings, to develop, test, and improve Zoom products and services, and to troubleshoot products and services. **Zoom does not use any of your audio, video, chat, screen sharing, attachments or other communications-like Customer Content (such as poll results, whiteboard and reactions) to train Zoom's or third-party artificial intelligence models.**
- **Marketing and Promotions:** To permit Zoom and/or its third party marketing partners to market, advertise, and promote Zoom products and services, including based on your product usage, information we receive from third-party partners, information you provide to process referral invitations, or if you visit our websites, information about how and when you visit, and your interactions with them. We may also use this information to provide advertisements to you relating to Zoom products and services or to engage third party partners to analyze your interactions on our website or app or to deliver advertising to you. Zoom does not use Customer Content for any marketing or promotions.
- **Authentication, Integrity, Security, and Safety:** To authenticate accounts and activity, detect, investigate, and prevent malicious conduct, fraudulent activity or unsafe experiences, address security threats, protect public safety, and secure Zoom products and services. Zoom uses advanced tools to automatically scan certain types of content such as virtual backgrounds, profile images, incoming emails to Zoom's native email service from someone who is not a Zoom Email user, and

files uploaded or exchanged through chat, for the purpose detecting and preventing violations of our terms or policies and illegal or other harmful activity.

- **Communicate with You:** We use personal data (including contact information) to communicate with you about Zoom products and services, including product updates, your account, and changes to our policies and terms. We also use your information to respond to you when you contact us.
- **Legal Reasons:** To comply with applicable law or respond to valid legal process, including from law enforcement or government agencies, to investigate or participate in civil discovery, litigation, or other adversarial legal proceedings, protect you, us, and others from fraudulent, malicious, deceptive, abusive, or unlawful activities, and to enforce or investigate potential violations of our Terms of Service or policies.

How Do We Share Personal Data?

Zoom provides personal data to third parties only with consent or in one of the following circumstances (subject to your prior consent where required under applicable law):

- **Resellers:** If an account owner licensed or purchased Zoom products and services from a third-party reseller of Zoom products and services, the reseller may be able to access personal data and content for users, including meetings, webinars, and messages hosted by the account owner.
- **Vendors:** Zoom works with third-party service providers to provide, support, and improve Zoom products and services and technical infrastructure, and for business services such as payment processing, including in relation to purchases made through the Zoom App Marketplace. Zoom may also work with third-party service providers to provide advertisements and business analytics regarding Zoom products and services. These vendors can access personal data subject to contractual and technical requirements for protecting personal data and prohibiting them from using personal data for any purpose other than to provide services to Zoom or as required by law. Zoom may integrate third-party technology to provide advanced features, such as Apple's TrueDepth technology, to process information on your device about your face or hand dimensions and gestures to provide video effects. This information is processed on your device, and such information is neither received nor stored by either the third party, or Zoom.
- **For Legal Reasons:** Zoom may share personal data as needed to: (1) comply with applicable law or respond to, investigate, or participate in valid legal process and proceedings, including from law enforcement or government agencies; (2) enforce or investigate potential violations of its Terms of Service or policies; (3) detect, prevent, or investigate potential fraud, abuse, or safety and security concerns, including threats to the public; (4) meet our corporate and social responsibility commitments; (5) protect our and our customers' rights and property; and (6) resolve disputes and enforce agreements.
- **Marketing, Advertising, and Analytics Partners:** Zoom uses third-party marketing, advertising, and analytics providers: to provide statistics and analysis about how people are using Zoom products and services, including our website; and to provide advertising and marketing for Zoom products and services, including targeted advertising based on your use of our website. These third-party partners may receive information about your activities on Zoom's website through third-party cookies placed on Zoom's website. To opt out of our use of third-party cookies that share data with these partners, visit our cookie management tool, available in Cookies Settings. Where required by law, Zoom will first obtain your consent before engaging in the marketing or advertising activities described.
- **Corporate Affiliates:** Zoom shares personal information with corporate affiliates, such as Zoom Voice Communications, Inc., to provide integrated and consistent experiences across Zoom products and services (such as enabling an account owner or their user to integrate a Zoom Phone call into a meeting) and to detect, investigate, and prevent fraud, abuse, and threats to public safety.

- **Change of Control:** We may share personal data with actual or prospective acquirers, their representatives and other relevant participants in, or during negotiations of, any sale, merger, acquisition, restructuring, or change in control involving all or a portion of Zoom's business or assets, including in connection with bankruptcy or similar proceedings.
- **Third-Party Developers:** If you purchase a third-party app or integration from the Zoom App Marketplace, Zoom may share information about the purchase with the third-party developer, to provide the app or integration.

Who Can See, Share, and Process My Personal Data When I Join Meetings and Use Other Zoom Products and Services?

When you send messages or join meetings and webinars on Zoom, other people and organizations, including third parties outside the meeting, webinar, or message, may be able to see content and information that you share:

- **Account Owner:** An account owner is the organization or individual that signs up for a Zoom account. Typically, an account owner designates one or more people (called an "administrator") to manage their account and can grant privileges to users on the account. Depending on their license with Zoom, the account owner can authorize additional users on their account, and the account owner can create and/or access the profile information for all users on their account. The account owner and their users can invite others (including guests not on their account and unlicensed participants) to meetings or webinars hosted on their account. Zoom gives account owners controls and features that they can use to determine whether certain types of content, such as recordings or Zoom Team Chat messages, can be created or sent, and what third-party apps can be used, for meetings and webinars hosted on their account. Depending on their settings, account owners and the users they designate can access personal data for participants who join meetings and webinars on their account or send messages to users on their account. Account owners may also be able to determine what information Zoom and others can access and use. Specifically, account owners may have access to:
 - **Account Usage:**
 - **Product Usage:** Information about how users and their devices interact with their account, which may include who sent messages to their users in chat, email addresses, IP addresses, device information, and other information about who joined meetings or webinars on their account, whether their users viewed or downloaded a recording, how long participants participated in their meetings, the time a message was sent, information about Zoom Phone integrations, and other usage information and feedback metrics.
 - **Participant List:** Information about the participants in a Zoom meeting, webinar, or chat, which may include name, display name, email address, phone number, and participant or user ID.
 - **Registration Information:** Information provided during registration for a webinar, meeting, Zoom Room, or recording hosted by the account.
 - **Zoom Team Chat and Out-of-Meeting Collaborations:** If enabled on their account, account owners and those they authorize can see information about who sent and received Zoom Team Chat messages, including synced in-meeting messages (e.g., from a dedicated meeting group chat that is synced with Zoom Team Chat), to users on their account, along with information about the message (for example, date and time, and number of members or participants). Depending on their settings, account owners also can see sender and receiver information, and other messaging data, along with the content of messages sent to and from users on their

account (including from in-meeting chat where dedicated meeting group chats are enabled), unless the account owner has enabled Advanced Chat Encryption. Depending on their settings, account owners and those they authorize may also see the content shared through collaborative features, including whiteboards, files, and images shared in Zoom Team Chat.

- **In-Meeting/Webinar Messages:** Depending on their settings, account owners can see sender and receiver information, along with the content of messages sent to and from users on their account, in the following circumstances:
 - Messages sent to Everyone in a meeting that is recorded
 - Messages sent to the meeting group chat in a meeting when a dedicated meeting group chat is enabled
 - Messages sent to panelists in a webinar that is recorded
 - Messages sent in dedicated meeting group chats in Team Chat
 - Direct messages if the account owner has enabled archiving
 - If a participant in a meeting is subject to archiving, their account owner will have access to messages sent to Everyone in the meeting, as well as direct messages sent to that participant. If a participant who is a member of a dedicated meeting group chat is subject to archiving, the member's account owner will have access to the meeting group chat messages, as well as direct messages sent to that member. If a guest in a meeting with a dedicated meeting group chat is subject to archiving, the guest's account owner will have access to messages sent to the meeting group chat, as well as direct messages sent to that guest.
- **Recordings:** Account owners can watch the content of recordings of meetings and webinars hosted on their account. They can also view, share, and enable advanced features for transcripts of meeting audio.
- **Polling, Q&A, and Feedback:** Account owners can see information about who provided responses to their polls, Q&A, or post meeting or webinar feedback requests, including name and contact information, together with the responses or feedback, unless responses are submitted anonymously.
- **Zoom Email and Zoom Calendar Content:** Depending on their settings, account owners, and designated account administrators, can access email and calendar content sent to and from users on their Zoom Email or Zoom Calendar accounts, even if those Zoom Emails are encrypted.
- **Meeting Hosts, Participants, and Invitees:** Meeting hosts, participants, and invitees may be able to see your email, display name, profile picture, and presence status, including in Zoom meetings and in Zoom's native calendar service. Meeting hosts, participants, and invitees can also see and (depending on the account owner's settings) record, save, and share meeting content, audio transcripts, messages sent to Everyone, messages sent to meeting group chats (where enabled, and whether sent in Team Chat or in-meeting), or messages sent to them directly, and files, whiteboards or other information shared with them (including during a meeting, or through a dedicated meeting group chat). Meeting hosts may also share chat transcripts to Zoom Team Chat, depending on their account owner's settings. Meeting hosts may also be able to see responses to Q&A and polls generated during the meeting.
- **Zoom Email, Calendar and Zoom Team Chat Recipients:** Recipients of Zoom Emails and Zoom Calendar invites can see, save, and share your email and calendar content with others, including by sharing emails to Zoom Team Chat. If a recipient shares encrypted content with others, for example, by sharing an encrypted Zoom Email to Zoom Team Chat, or forwarding an encrypted Zoom Email to a third-party recipient without a Zoom Email account, the shared or forwarded content will not be end-to-end encrypted by Zoom. Those with access to your device and login credentials may be able to see, save and share your email and calendar contents on that device. Recipients of Zoom Team Chats can see your messages, reactions, emojis, and related content, including content from

Zoom Emails, Zoom Calendar, and emails from third-party services integrated in the Zoom client, that you or a third-party choose to share to Zoom Team Chat, and in-meeting messages that participants send that are synced with Zoom Team Chat through dedicated meeting group chats. Depending on the account owner's settings, Zoom Team Chat recipients may record, save, or share your messages.

- **Webinar Panelists and Attendees:** Only panelists may be visible to attendees during a webinar, but attendees who agree to unmute can be heard by other attendees. If an attendee agrees to become a panelist during a webinar, they may be visible to other attendees, depending on settings. Panelists and attendees may be able to see the name of a participant who asks a question during a Q&A, along with their question, unless the participant submits the question anonymously.
- **Livestreams:** Meeting and webinar hosts can choose to livestream to a third-party site or service, which means anyone with access to the livestream will be able to see the meeting or webinar.
- **Apps and Integrations:**
 - Account owners can choose to add Zoom-developed apps and third-party apps to their account and the Zoom products they use, including via use of the Zoom App Marketplace, and they can also control whether their users can add and use specific Zoom and third-party apps, including in meetings, webinars, and chats hosted on their account.
 - Account owners can also choose to integrate other content from third-party services— such as third-party email communications on their corporate account – to apps and services that they use, such as Zoom Revenue Accelerator (that provides insights and business analytics related to businesses when they use Zoom products). Further, account owners may choose to have Zoom analyze the meeting's audio recording to distinguish one speaker from another in order to create an accurate transcript. The audio analysis is not retained after the transcript is generated.
 - Depending on their settings, account owners', users' and guests' personal data and content may be shared with apps and integrations, including Zoom-developed apps, approved by account owners, which may include all of the personal data categories listed above, such as account information, profile and contact information, registration information, participants list, settings, content, product usage, device information, or third-party emails that have been shared with the app.
 - Other participants in the meeting may be able to see the app that you are using in a meeting, if the app is receiving content (including audio and video) from the meeting.
 - Third-party developers may also integrate or embed Zoom meetings into their website or app experiences or build versions of Zoom that enable access to Zoom products from a third-party app.
 - Personal information shared by account owners and users with third-party apps and integrations is collected and processed in accordance with the app developers' terms and privacy policies, not Zoom's.

Privacy Rights and Choices

Marketing Communications

If you don't want to learn about products and services we or our partners offer, you can opt-out of marketing communications in the communication sent to you (for example, via email or SMS), or by emailing privacy@zoom.us. Not all of our communications are for marketing, and you'll continue to receive messages related to your products and services, such as bills, transactional notices, or customer service.

Data Rights

If you are in the [European Economic Area \(EEA\), Switzerland, or the UK](#), or a resident of [California or](#)

[another U.S. state](#) with an applicable privacy law, please refer to the respective dedicated sections below. Otherwise, at your request, and as required by applicable law, we will:

- Inform you of what personal data we have about you that is under our control;
- Amend or correct such personal data or any previous privacy preferences you selected, or direct you to applicable tools; and/or
- Delete such personal data or direct you to applicable tools.

In order to exercise any of your rights as to personal data controlled by Zoom, please [click here](#). Where legally permitted, we may decline to process requests that are unreasonably repetitive or systematic, require disproportionate technical effort, or jeopardize the privacy of others. As an account owner or a user under a licensed account, you may also take steps to affect your personal data by visiting your account and modifying your personal data directly.

Children

Zoom does not allow children under the age of 16 to sign up for a Zoom account.

For educational organizations that use Zoom products and services to provide educational services to children under 18, Zoom's Children's Educational Privacy Statement is available [here](#).

How to Contact Us

To exercise your rights, please [click here](#). If you have any privacy-related questions or comments related to this Privacy Statement, please send an email to privacy@zoom.us.

You can also contact us by writing to the following address:

Zoom Video Communications, Inc.
Attention: Data Protection Officer
55 Almaden Blvd, Suite 600
San Jose, CA 95113

Or to our representative in the EU or UK:

Lionheart Squared Ltd
Attn: Data Privacy
2 Pembroke House
Upper Pembroke Street 28-32
Dublin
DO2 EK84
Republic of Ireland
email: zoom@LionheartSquared.eu

Lionheart Squared Limited
Attn: Data Privacy
17 Glasshouse Studios
Fryern Court Road
Fordingbridge
Hampshire
SP6 1QX

United Kingdom
Contact: zoom@LionheartSquared.co.uk

You can contact our Data Protection Officer by sending an email to privacy@zoom.us.

Retention

We retain personal data for as long as required to engage in the uses described in this Privacy Statement, unless a longer retention period is required by applicable law.

The criteria used to determine our retention periods include the following:

- The length of time we have an ongoing relationship with you and provide Zoom products and services to you (for example, for as long as you have an account with us or keep using our products);
- Whether account owners modify or their users delete information through their accounts;
- Whether we have a legal obligation to keep the data (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them); or
- Whether retention is advisable in light of our legal position (such as in regard to the enforcement of our agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation).

European Data Protection Specific Information

Data Subjects Rights

If you are in the EEA, Switzerland, or the UK, your rights in relation to your personal data processed by us as a controller specifically include:

- **Right of access and/or portability:** You have the right to access any personal data that we hold about you and, in some circumstances, have that data provided to you so that you can provide or “port” that data to another provider;
- **Right of erasure:** In certain circumstances, you have the right to the erasure of personal data that we hold about you (for example, if it is no longer necessary for the purposes for which it was originally collected);
- **Right to object to processing:** In certain circumstances, you have the right to request that we stop processing your personal data and/or stop sending you marketing communications;
- **Right to rectification:** You have the right to require us to correct any inaccurate or incomplete personal data;
- **Right to restrict processing:** You have the right to request that we restrict processing of your personal data in certain circumstances (for example, where you believe that the personal data we hold about you is not accurate or lawfully held).

To exercise your rights, please [click here](#). If you have any other questions about our use of your personal data, please send a request at the contact details specified in the How to Contact Us section of this Privacy Statement. Please note that we may request you to provide us with additional information in order to confirm your identity and ensure that you are entitled to access the relevant personal data.

You also have the right to lodge a complaint to a data protection authority. For more information, please contact your local data protection authority.

Legal Basis for Processing Personal Data

We only use your information in a lawful, transparent, and fair manner. Depending on the specific personal data concerned and the factual context, when Zoom processes personal data as a controller for individuals in regions such as the EEA, Switzerland, and the UK, we rely on the following legal bases as applicable in your jurisdiction:

- **As necessary for our contract:** When we enter into a contract directly with you, we process your personal data on the basis of our contract in order to prepare and enter into the contract, as well as to perform and manage our contract (i.e., providing Zoom products and services, features and services to account owners, their users, and those they invite to join meetings and webinars hosted on their accounts, and manage our relationship and contract, including billing, compliance with contractual obligations, and related administration). If we do not process your personal data for these purposes, we may not be able to provide you with all products and services;
- **Consistent with specific revocable consents:** We rely on your prior consent in order to utilize cookies to engage advertising and analytics partners to deliver tailored advertising and analysis of our website usage. You have the right to withdraw your consent at any time by visiting our cookie management tool, available Cookies Settings;
- **As necessary to comply with our legal obligations:** We process your personal data to comply with the legal obligations to which we are subject for the purposes of compliance with EEA laws, regulations, codes of practice, guidelines, or rules applicable to us, and for responses to requests from, and other communications with, competent EEA public, governmental, judicial, or other regulatory authorities. This includes detecting, investigating, preventing, and stopping fraudulent, harmful, unauthorized, or illegal activity (“fraud and abuse detection”) and compliance with privacy laws;
- **To protect your vital interests or those of others:** We process certain personal data in order to protect vital interests for the purpose of detecting and preventing illicit activities that impact vital interests and public safety, including child sexual abuse material; and
- **As necessary for our (or others’) legitimate interests, unless those interests are overridden by your interests or fundamental rights and freedoms, which require protection of personal data:** We process your personal data based on such legitimate interests to (i) enter and perform the contract with the account owner and/or reseller providing you with the products and services (which includes billing, compliance with contractual obligations, and related administration and support); (ii) develop, test, and improve our products and services and troubleshoot products and services; (iii) ensure authentication, integrity, security, and safety of accounts, activity, and products and services, including detect and prevent malicious conduct and violations of our terms and policies, prevent or investigate bad or unsafe experiences, and address security threats; (iv) send marketing communications, advertising, and promotions related to the products and services; and (v) comply with non-EEA laws, regulations, codes of practice, guidelines, or rules applicable to us and respond to requests from, and other communications with, competent non-EEA public, governmental, judicial, or other regulatory authorities, as well as meet our corporate and social responsibility commitments, protect our rights and property and the ones of our customers, resolve disputes, and enforce agreements.

International Data Transfers

Zoom operates globally, which means personal data may be transferred, stored (for example, in a data center), and processed outside of the country or region where it was initially collected where Zoom or its service providers have customers or facilities – including in countries where meeting participants or account owners hosting meetings or webinars that you participate in or receiving messages that you send are based.

Therefore, by using Zoom products and services or providing personal data for any of the purposes stated above, you acknowledge that your personal data may be transferred to or stored in the United States where we are established, as well as in other countries outside of the EEA, Switzerland, and the UK. Such countries may have data protection rules that are different and less protective than those of your country.

We protect your personal data in accordance with this Privacy Statement wherever it is processed and take appropriate contractual or other steps to protect it under applicable laws. Where personal data of users in the EEA, Switzerland, or the UK is being transferred to a recipient located in a country outside the EEA, Switzerland, or the UK which has not been recognized as having an adequate level of data protection, we ensure that the transfer is governed by the European Commission's standard contractual clauses. Please contact us if you would like further information in that respect.

California & Other U.S. States Notice at Collection

Categories of Personal Information Zoom Receives: Zoom may collect, or process on behalf of our customers, the following categories of personal data, as described above, in the "What Personal Data Do We Receive?" section: identifiers (such as in Account Information, Profile and Participant Information, Contact Information, and Registration Information), financial account information (such as in Account Information); commercial information (such as in Account Information); internet or other electronic network activity information (such as Device Information, Usage Information Regarding Meetings, Webinars, Message, Collaborative Features, and the Website, and Limited Information from Zoom Email and Calendar Services); audio, electronic, and visual information (such as in Content and Context from Meetings, Webinars, Messaging, and Other Collaborative Features) education information such as from university customers; inferences we derive from the preceding or other information we collect; and sensitive personal information (such as certain categories in Account Information, Content and Context from Meetings, Webinars, Messaging, and Other Collaborative Features).

Sources: We receive information from sources as described in the "What Personal Data Do We Receive?" section, including: from you (including through your use of our products and services); from partners; from customers; and from publicly available sources. We collect education information from schools that use our services. Please see our Children's Educational Privacy Statement for more information.

Zoom's business and commercial purposes for use: Zoom uses personal data for the following business and commercial purposes: to provide Zoom Products and Services; for Product Research and Development; for Marketing and Promotions (Zoom does not use meeting, webinar, or messaging content, or any content generated or shared as part of other collaborative features for any marketing or promotions); Authentication, Integrity, Security, and Safety; to Communicate with You; and for Legal Reasons. For more information, please see "How We Share Personal Data?" Categories of third parties to whom we disclose Personal Information for business purposes are described in "How We Share Personal Data?"

Zoom may permit advertising and analytics services that are intended to deliver advertising to you and/or analyze your interactions, based on your interactions with our website or app which may constitute a "sale" or "sharing" of data for targeted advertising purposes under certain state privacy laws. See "California & Other U.S. State Privacy Rights" for more information regarding your right to opt-out.

Retention: Zoom retains personal data for as long as required to engage in the uses described in this Privacy Statement, unless a longer retention period is required by applicable law. Additional detail on

retention criteria can be found under Retention, above.

California & Other U.S. State Privacy Rights

Under some U.S. state laws, including the California Consumer Privacy Act of 2018 (as amended by the California Consumer Privacy Rights Act) (CCPA), residents may have a right to:

- **Access** the categories and specific pieces of personal data Zoom has collected, the categories of sources from which the personal data is collected, the business purpose(s) for collecting the personal data, and the categories of third parties with whom Zoom has shared personal data, and obtain the personal data in a portable and, to the extent technically feasible, readily usable format;
- **Delete** personal data under certain circumstances;
- **Correct** personal data under certain circumstances; and
- **Opt out of the “sale” of personal data or “sharing” of personal data for targeted advertising purposes.** We do not sell your personal data in the conventional sense. However, like many companies, we may use advertising and analytics services that are intended to analyze your interactions with our website or app, based on information obtained from cookies or other trackers, including for delivering advertising to you (such as interest-based, targeted, or cross-context behavioral advertising). You can get more information and opt out of the use of cookies and other trackers on our website and app by clicking the Cookies Settings/Your Privacy Choices link, also on our homepage, and setting your preferences. You will need to set your preferences from each device and each web browser from which you wish to opt out. This feature uses a cookie to remember your preference, so if you clear all cookies from your browser, you will need to re-select your preferred settings. California and Connecticut residents may also set the Global Privacy Control (GPC) to opt out of the “sale” or “sharing” of your personal information for targeted advertising for each participating browser system that you use. Zoom does not have actual knowledge that it “sells” or “shares” the personal information of consumers under 16 years of age.
- **Appeal** a denial of your request. Some states provide additional rights to their residents. If we decline to process your request, you may have the right to appeal our decision. You can do so by replying directly to our denial or emailing privacy@zoom.us.

Zoom will not discriminate against you for exercising any of these rights, which is further in line with your rights under state law.

Sensitive Information. Zoom receives information that may be considered sensitive under some state laws, such as certain Account Information (e.g., financial information, log-in information), certain Content and Context from Meetings, Webinars, Messaging, and Other Collaborative Features and certain Limited Information from Zoom Email and Calendar Services (e.g., messaging content in cases described herein). Zoom processes sensitive personal information to provide Zoom products and services, for product research and development, for authentication, integrity, security, and safety reasons, to communicate with you, for legal reasons, and with your consent. Zoom does not use or disclose sensitive personal information (as defined under CCPA) for purposes of inferring characteristics about a consumer, or in any way that would require Zoom to provide a right to limit under the CCPA. Under certain laws, residents may also be permitted to opt out of certain profiling relating to automated processing analyzing certain categories of an individual's information that would produce a legal or similarly significant effect. Zoom does not engage in this type of profiling of individuals.

To exercise your rights, please click [here](#) or call +1-888-799-0566. To opt out of the use of cookies on our sites for interest-based advertising purposes, follow the instructions above.

We will acknowledge receipt of your request within 10 business days, and provide a substantive response within 45 calendar days, or inform you of the reason and extension period (up to a total of 90 days) in writing.

These rights are not absolute, are subject to exceptions and limitations, and may not be afforded to residents of all states. In certain cases, we may decline requests to exercise these rights where permitted by law. We will need to verify your identity to process your access, deletion, and correction requests and reserve the right to confirm your state residency. To verify your identity, we may require you to log into your existing Zoom account (if applicable), give a declaration as to your identity under penalty of perjury, and/or provide additional information, such as providing at least two pieces of personal information relating to your account (which will be compared to information we have, such as profile information) or as we otherwise may already have in our possession, such as your email address and phone number. We will verify your consumer request by comparing the information you provide to information already in our possession, and take additional steps to minimize the risk of fraud. You may designate an authorized agent to submit your verified consumer request by providing written permission and verifying your identity, or through proof of power of attorney.

To see our Disclosure of Privacy Rights Requests, please [click here](#).

California's Shine the Light Law

California Civil Code Section 1798.83, also known as "Shine The Light" law, permits California residents to annually request information regarding the disclosure of your Personal Information (if any) to third parties for the third parties' direct marketing purposes in the preceding calendar year. We do not share Personal Information with third parties for the third parties' direct marketing purposes.

Changes to This Privacy Statement

We may update this Privacy Statement periodically to account for changes in our collection and/or processing of personal data, and will post the updated Privacy Statement on our website, with a "Last Updated" date at the top. If we make material changes to this Privacy Statement, we will notify you and provide you an opportunity to review before you choose to continue using our products and services.

[About](#)

[Zoom Blog](#)

[Customers](#)

[Our Team](#)

[Careers](#)

[Integrations](#)

[Partners](#)

[Investors](#)

[Press](#)

Zoom Privacy Statement

Last updated: August 11, 2023

This Privacy Statement describes the personal data we collect and/or process (which may include collecting, organizing, structuring, storing, using, or disclosing) to provide products and services offered directly by Zoom Video Communications, Inc. (“Zoom”), including Zoom’s websites, its meetings, webinars, and messaging platform, related collaborative features, and Zoom App Marketplace (“Zoom products and services” or “products and services”). Zoom products and services covered in this Privacy Statement do not include products or services developed by Zoom that are covered under a separate privacy policy (including those listed here).

California residents, please see our California Privacy Notice at Collection, and California & Other U.S. State Privacy Rights sections.

[What Personal Data Do We Receive?](#)

[How Do We Use Personal Data?](#)

[How Do We Share Personal Data?](#)

[Who Can See, Share, and Process My Personal Data When I Join Meetings and Use Other Zoom Products and Services?](#)

[Privacy Rights and Choices](#)

[Children](#)

[How to Contact Us](#)

[Retention](#)

[European Data Protection Specific Information](#)

[California & Other U.S. States Notice at Collection](#)

[California & Other U.S. State Privacy Rights](#)

[Changes to This Privacy Statement](#)

What Personal Data Do We Receive?

Personal data is any information from or about an identified or identifiable person, including information that Zoom can associate with an individual person. We may collect, or process on behalf of our customers, the following categories of personal data when you use or interact with Zoom products and services:

- **Account Information:** Information associated with an account that licenses Zoom products and services, which may include administrator name, contact information, account ID, billing and transaction information, and account plan information.
- **Profile and Participant Information:** Information associated with the Zoom profile of a user who uses Zoom products and services under a licensed account or that is provided by an unlicensed participant joining a meeting, which may include name, display name, picture, email address, phone number, job information, stated locale, user ID, or other information provided by the user and/or their account owner.
- **Contact Information:** Contact information added by accounts and/or their users to create contact lists on Zoom products and services, which may include contact information a user integrates from a third-party app, or provided by users to process referral invitations.
- **Settings:** Information associated with the preferences and settings on a Zoom account or user profile, which may include audio and video settings, recording file location, screen sharing settings, and other settings and configuration information.
- **Registration Information:** Information provided when registering for a Zoom meeting, webinar, Zoom Room, or recording, which may include name and contact information, responses to registration questions, and other registration information requested by the host.
- **Device Information:** Information about the computers, phones, and other devices used when interacting with Zoom products and services, which may include information about the speakers, microphone, camera, OS version, hard disk ID, PC name, MAC address, IP address (which may be used to infer general location at a city or country level), device attributes (like operating system version and battery level), WiFi information, and other device information (like Bluetooth signals).
- **Content and Context from Meetings, Webinars, Messaging, and Other Collaborative Features:** Content generated in meetings, webinars, or messages that are hosted on Zoom products and services ("Customer Content"), which may include audio, video, in-meeting messages, in-meeting and out-of-meeting whiteboards, chat messaging content, transcriptions, transcript edits and recommendations, written feedback, responses to polls and Q&A, and files, as well as related context, such as invitation details, meeting or chat name, or meeting agenda. Customer Content may contain your voice and image, depending on the account owner's settings, what you choose to share, your settings, and what you do on Zoom products and services. As referenced below, Zoom employees do not access or use Customer Content without the authorization of the hosting account owner, or as required for legal, safety, or security reasons.
- **Usage Information Regarding Meetings, Webinars, Messaging, Collaborative Features and the Website:** Information about how people and their devices interact with Zoom products and services, such as: when participants join and leave a meeting; whether participants sent messages and who they message with; performance data; mouse movements, clicks, keystrokes or actions (such as mute/unmute or video on/off), edits to transcript text, where authorized by the account owner and other inputs that help Zoom to understand feature usage, improve product design, and suggest features; which third-party apps are added to a meeting or other product or service and what information and actions the app is authorized to access and perform; use of third-party apps and the Zoom App Marketplace; features used (such as screen sharing, emojis, or filters); and other usage information and metrics. This also includes information about when and how people visit and interact with Zoom's websites, including what pages are accessed, interaction with website features

including Zoom's website's virtual chat feature, and whether or not the person signed up for a Zoom product or service.

- **Limited Information from Zoom Email and Calendar Services:** "Zoom Email" refers to Zoom's native email service and emails sent from Zoom's native email service. Zoom Email is designed to be end-to-end encrypted by Zoom by default for emails sent and received directly between active Zoom Email users. Support for end-to-end encryption requires Zoom Email users to have added a device to their Zoom Email account with the associated email address and to use a supported Zoom client. When an email is end-to-end encrypted, only the users, and, depending on their settings, account owners, or designated account administrators control the encryption key and therefore access to the email content, including body text, subject line, attachments and custom labels applied to messages by users in their inboxes. Emails sent to or received from non-Zoom Email users are encrypted after the email is sent or received from Zoom's servers, if the Zoom Email user chooses to send them with encryption. In all cases, Zoom does not have access to email metadata used for basic email delivery—specifically, email addresses in the from, to, cc, and bcc fields, time, mimeType, and the number and size of attachments. From use of Zoom's native calendar service, Zoom receives information regarding meeting invitations, body text, sender and recipients, and other calendar information.
- **Content from Third-Party Integrations:** Users can access email and calendars from third-party services through their Zoom client, if they choose to integrate them. This information is not end-to-end encrypted by Zoom, but Zoom employees do not access the contents of third-party-service email or calendar entries, unless authorized to, or required for legal, safety, or security reasons. If account owners and/or their licensed end users integrate their third-party emails with products and services offered or powered by Zoom, such as business analytics tools like Zoom Revenue Accelerator Zoom may collect or process Customer Content and email information, including email content, headers and metadata, from such third-party services.
- **Communications with Zoom:** Information about, and contents of, your communications with Zoom, including relating to support questions, website virtual chats, your account, and other inquiries.
- **Information from Partners:** Zoom obtains information about account owners and their users from third-party companies, such as market data enrichment services, including information about an account owner's company size or industry, contact information, or activity of certain enterprise domains. Zoom may also obtain information from third-party advertising partners that deliver ads displayed on Zoom products and services, such as whether you clicked on an ad they showed you.

In certain jurisdictions, some of the personal data Zoom receives may be considered sensitive. Please see "California & Other U.S. State Privacy Rights" for more information.

How Do We Use Personal Data?

Zoom employees do not access or use Customer Content including meeting, webinar, messaging, or email content (specifically, audio, video, files, in-meeting whiteboards, messaging, or email contents), or any content generated or shared as part of other collaborative features (such as out-of-meeting whiteboards), unless authorized by the account owner hosting the Zoom product or service where the Customer Content was generated, or as required for legal, safety, or security reasons. **Zoom does not use any of your audio, video, chat, screen sharing, attachments or other communications-like Customer Content (such as poll results, whiteboard and reactions) to train Zoom's or third-party artificial intelligence models.**

As discussed below, and where technically feasible, Zoom uses personal data to conduct the following activities:

- **Provide Zoom Products and Services:** To provide and develop products and services to account owners, their licensed end users, and those they invite to join meetings and webinars hosted on

their accounts, including to customize Zoom products and services and recommendations for accounts or their users. Zoom also uses personal data to determine what products and services may be available in your location, and uses personal data, including contact information, to route invitations, messages, or Zoom Emails to recipients when users send or receive invitations, messages, or Zoom Emails using Zoom products and services. This may also include using personal data for customer support, which may include accessing audio, video, files, messages, and other content or context, at the direction of the account owner or their users. We also use personal data to manage our relationships and contracts with account owners and others, including billing, compliance with contractual obligations, facilitating payment to third-party developers in relation to purchases made through the Zoom App Marketplace, and related administration.

- **Advanced Audio and Video Features:** If you elect to turn on certain video features, if available in your area, such as filters, studio effects, avatars, and gestures, information about your movements or the positioning of your face or hands may be processed on your device to apply the selected features. Such data does not leave your device, is not retained, cannot be used to identify you, and is only used to generate the selected effects. If certain other features are enabled by the account owner hosting a Zoom product or service, such as transcription generation for recordings, Zoom may use technology that analyzes the meeting's audio recording to distinguish one speaker from another in order to create an accurate transcript. The audio analysis is not retained after the transcript is generated.
 - If you elect to turn on personalized audio isolation, software on your device will capture and analyze a clip of your audio from meetings you join to create an Audio Signature used to differentiate your voice from, and suppress background noise in, meetings you join. Zoom does not receive or retain the clip or Audio Signature, which stays on your device and is only used for noise suppression in meetings you join. You may delete the Audio Signature from your device through your Zoom app settings.
- **Intelligent Features:** If enabled by the account owner, Zoom provides intelligent features and products to its customers, their licensed end users and guests, such as Zoom AI Companion or other tools to recommend chat, email or other content. These tools may use artificial intelligence, machine learning, or other technology to process Customer Content solely to provide the intelligent features.
- **Product Research and Development:** If authorized by any applicable customer settings, to develop, test, and improve Zoom products and services, and to troubleshoot products and services. **Zoom does not use any of your audio, video, chat, screen sharing, attachments or other communications-like Customer Content (such as poll results, whiteboard and reactions) to train Zoom's or third-party artificial intelligence models.**
- **Marketing and Promotions:** To permit Zoom and/or its third party marketing partners to market, advertise, and promote Zoom products and services, including based on your product usage, information we receive from third-party partners, information you provide to process referral invitations, or if you visit our websites, information about how and when you visit, and your interactions with them. We may also use this information to provide advertisements to you relating to Zoom products and services or to engage third party partners to analyze your interactions on our website or app or to deliver advertising to you. Zoom does not use Customer Content for any marketing or promotions.
- **Authentication, Integrity, Security, and Safety:** To authenticate accounts and activity, detect, investigate, and prevent malicious conduct, fraudulent activity or unsafe experiences, address security threats, protect public safety, and secure Zoom products and services. Zoom uses advanced tools to automatically scan certain types of content such as virtual backgrounds, profile images, incoming emails to Zoom's native email service from someone who is not a Zoom Email user, and

files uploaded or exchanged through chat, for the purpose detecting and preventing violations of our terms or policies and illegal or other harmful activity.

- **Communicate with You:** We use personal data (including contact information) to communicate with you about Zoom products and services, including product updates, your account, and changes to our policies and terms. We also use your information to respond to you when you contact us.
- **Legal Reasons:** To comply with applicable law or respond to valid legal process, including from law enforcement or government agencies, to investigate or participate in civil discovery, litigation, or other adversarial legal proceedings, protect you, us, and others from fraudulent, malicious, deceptive, abusive, or unlawful activities, and to enforce or investigate potential violations of our Terms of Service or policies.

How Do We Share Personal Data?

Zoom provides personal data to third parties only with consent or in one of the following circumstances (subject to your prior consent where required under applicable law):

- **Resellers:** If an account owner licensed or purchased Zoom products and services from a third-party reseller of Zoom products and services, the reseller may be able to access personal data and content for users, including meetings, webinars, and messages hosted by the account owner.
- **Vendors:** Zoom works with third-party service providers to provide, support, and improve Zoom products and services and technical infrastructure, and for business services such as payment processing, including in relation to purchases made through the Zoom App Marketplace. Zoom may also work with third-party service providers to provide advertisements and business analytics regarding Zoom products and services. These vendors can access personal data subject to contractual and technical requirements for protecting personal data and prohibiting them from using personal data for any purpose other than to provide services to Zoom or as required by law. Zoom may integrate third-party technology to provide advanced features, such as Apple's TrueDepth technology, to process information on your device about your face or hand dimensions and gestures to provide video effects. This information is processed on your device, and such information is neither received nor stored by either the third party, or Zoom.
- **For Legal Reasons:** Zoom may share personal data as needed to: (1) comply with applicable law or respond to, investigate, or participate in valid legal process and proceedings, including from law enforcement or government agencies; (2) enforce or investigate potential violations of its Terms of Service or policies; (3) detect, prevent, or investigate potential fraud, abuse, or safety and security concerns, including threats to the public; (4) meet our corporate and social responsibility commitments; (5) protect our and our customers' rights and property; and (6) resolve disputes and enforce agreements.
- **Marketing, Advertising, and Analytics Partners:** Zoom uses third-party marketing, advertising, and analytics providers: to provide statistics and analysis about how people are using Zoom products and services, including our website; and to provide advertising and marketing for Zoom products and services, including targeted advertising based on your use of our website. These third-party partners may receive information about your activities on Zoom's website through third-party cookies placed on Zoom's website. To opt out of our use of third-party cookies that share data with these partners, visit our cookie management tool, available in Cookies Settings. Where required by law, Zoom will first obtain your consent before engaging in the marketing or advertising activities described.
- **Corporate Affiliates:** Zoom shares personal information with corporate affiliates, such as Zoom Voice Communications, Inc., to provide integrated and consistent experiences across Zoom products and services (such as enabling an account owner or their user to integrate a Zoom Phone call into a meeting) and to detect, investigate, and prevent fraud, abuse, and threats to public safety.

- **Change of Control:** We may share personal data with actual or prospective acquirers, their representatives and other relevant participants in, or during negotiations of, any sale, merger, acquisition, restructuring, or change in control involving all or a portion of Zoom's business or assets, including in connection with bankruptcy or similar proceedings.
- **Third-Party Developers:** If you purchase a third-party app or integration from the Zoom App Marketplace, Zoom may share information about the purchase with the third-party developer, to provide the app or integration.

Who Can See, Share, and Process My Personal Data When I Join Meetings and Use Other Zoom Products and Services?

When you send messages or join meetings and webinars on Zoom, other people and organizations, including third parties outside the meeting, webinar, or message, may be able to see content and information that you share:

- **Account Owner:** An account owner is the organization or individual that signs up for a Zoom account. Typically, an account owner designates one or more people (called an "administrator") to manage their account and can grant privileges to users on the account. Depending on their license with Zoom, the account owner can authorize additional users on their account, and the account owner can create and/or access the profile information for all users on their account. The account owner and their users can invite others (including guests not on their account and unlicensed participants) to meetings or webinars hosted on their account. Zoom gives account owners controls and features that they can use to determine whether certain types of content, such as recordings or Zoom Team Chat messages, can be created or sent, and what third-party apps can be used, for meetings and webinars hosted on their account. Depending on their settings, account owners and the users they designate can access personal data for participants who join meetings and webinars on their account or send messages to users on their account. Account owners may also be able to determine what information Zoom and others can access and use. Specifically, account owners may have access to:
 - **Account Usage:**
 - **Product Usage:** Information about how users and their devices interact with their account, which may include who sent messages to their users in chat, email addresses, IP addresses, device information, and other information about who joined meetings or webinars on their account, whether their users viewed or downloaded a recording, how long participants participated in their meetings, the time a message was sent, information about Zoom Phone integrations, and other usage information and feedback metrics.
 - **Participant List:** Information about the participants in a Zoom meeting, webinar, or chat, which may include name, display name, email address, phone number, and participant or user ID.
 - **Registration Information:** Information provided during registration for a webinar, meeting, Zoom Room, or recording hosted by the account.
 - **Zoom Team Chat and Out-of-Meeting Collaborations:** If enabled on their account, account owners and those they authorize can see information about who sent and received Zoom Team Chat messages, including synced in-meeting messages (e.g., from a dedicated meeting group chat that is synced with Zoom Team Chat), to users on their account, along with information about the message (for example, date and time, and number of members or participants). Depending on their settings, account owners also can see sender and receiver information, and other messaging data, along with the content of messages sent to and from users on their

account (including from in-meeting chat where dedicated meeting group chats are enabled), unless the account owner has enabled Advanced Chat Encryption. Depending on their settings, account owners and those they authorize may also see the content shared through collaborative features, including whiteboards, files, and images shared in Zoom Team Chat.

- **In-Meeting/Webinar Messages:** Depending on their settings, account owners can see sender and receiver information, along with the content of messages sent to and from users on their account, in the following circumstances:
 - Messages sent to Everyone in a meeting that is recorded
 - Messages sent to the meeting group chat in a meeting when a dedicated meeting group chat is enabled
 - Messages sent to panelists in a webinar that is recorded
 - Messages sent in dedicated meeting group chats in Team Chat
 - Direct messages if the account owner has enabled archiving
 - If a participant in a meeting is subject to archiving, their account owner will have access to messages sent to Everyone in the meeting, as well as direct messages sent to that participant. If a participant who is a member of a dedicated meeting group chat is subject to archiving, the member's account owner will have access to the meeting group chat messages, as well as direct messages sent to that member. If a guest in a meeting with a dedicated meeting group chat is subject to archiving, the guest's account owner will have access to messages sent to the meeting group chat, as well as direct messages sent to that guest.
- **Recordings:** Account owners can watch the content of recordings of meetings and webinars hosted on their account. They can also view, share, and enable advanced features for transcripts of meeting audio.
- **Polling, Q&A, and Feedback:** Account owners can see information about who provided responses to their polls, Q&A, or post meeting or webinar feedback requests, including name and contact information, together with the responses or feedback, unless responses are submitted anonymously.
- **Zoom Email and Zoom Calendar Content:** Depending on their settings, account owners, and designated account administrators, can access email and calendar content sent to and from users on their Zoom Email or Zoom Calendar accounts, even if those Zoom Emails are encrypted.
- **Meeting Hosts, Participants, and Invitees:** Meeting hosts, participants, and invitees may be able to see your email, display name, profile picture, and presence status, including in Zoom meetings and in Zoom's native calendar service. Meeting hosts, participants, and invitees can also see and (depending on the account owner's settings) record, save, and share meeting content, audio transcripts, messages sent to Everyone, messages sent to meeting group chats (where enabled, and whether sent in Team Chat or in-meeting), or messages sent to them directly, and files, whiteboards or other information shared with them (including during a meeting, or through a dedicated meeting group chat). Meeting hosts may also share chat transcripts to Zoom Team Chat, depending on their account owner's settings. Meeting hosts may also be able to see responses to Q&A and polls generated during the meeting.
- **Zoom Email, Calendar and Zoom Team Chat Recipients:** Recipients of Zoom Emails and Zoom Calendar invites can see, save, and share your email and calendar content with others, including by sharing emails to Zoom Team Chat. If a recipient shares encrypted content with others, for example, by sharing an encrypted Zoom Email to Zoom Team Chat, or forwarding an encrypted Zoom Email to a third-party recipient without a Zoom Email account, the shared or forwarded content will not be end-to-end encrypted by Zoom. Those with access to your device and login credentials may be able to see, save and share your email and calendar contents on that device. Recipients of Zoom Team Chats can see your messages, reactions, emojis, and related content, including content from

Zoom Emails, Zoom Calendar, and emails from third-party services integrated in the Zoom client, that you or a third-party choose to share to Zoom Team Chat, and in-meeting messages that participants send that are synced with Zoom Team Chat through dedicated meeting group chats. Depending on the account owner's settings, Zoom Team Chat recipients may record, save, or share your messages.

- **Webinar Panelists and Attendees:** Only panelists may be visible to attendees during a webinar, but attendees who agree to unmute can be heard by other attendees. If an attendee agrees to become a panelist during a webinar, they may be visible to other attendees, depending on settings. Panelists and attendees may be able to see the name of a participant who asks a question during a Q&A, along with their question, unless the participant submits the question anonymously.
- **Livestreams:** Meeting and webinar hosts can choose to livestream to a third-party site or service, which means anyone with access to the livestream will be able to see the meeting or webinar.
- **Apps and Integrations:**
 - Account owners can choose to add Zoom-developed apps and third-party apps to their account and the Zoom products they use, including via use of the Zoom App Marketplace, and they can also control whether their users can add and use specific Zoom and third-party apps, including in meetings, webinars, and chats hosted on their account.
 - Account owners can also choose to integrate other content from third-party services— such as third-party email communications on their corporate account – to apps and services that they use, such as Zoom Revenue Accelerator (that provides insights and business analytics related to businesses when they use Zoom products). Further, account owners may choose to have Zoom analyze the meeting's audio recording to distinguish one speaker from another in order to create an accurate transcript. The audio analysis is not retained after the transcript is generated.
 - Depending on their settings, account owners', users' and guests' personal data and content may be shared with apps and integrations, including Zoom-developed apps, approved by account owners, which may include all of the personal data categories listed above, such as account information, profile and contact information, registration information, participants list, settings, content, product usage, device information, or third-party emails that have been shared with the app.
 - Other participants in the meeting may be able to see the app that you are using in a meeting, if the app is receiving content (including audio and video) from the meeting.
 - Third-party developers may also integrate or embed Zoom meetings into their website or app experiences or build versions of Zoom that enable access to Zoom products from a third-party app.
 - Personal information shared by account owners and users with third-party apps and integrations is collected and processed in accordance with the app developers' terms and privacy policies, not Zoom's.

Privacy Rights and Choices

Marketing Communications

If you don't want to learn about products and services we or our partners offer, you can opt-out of marketing communications in the communication sent to you (for example, via email or SMS), or by emailing privacy@zoom.us. Not all of our communications are for marketing, and you'll continue to receive messages related to your products and services, such as bills, transactional notices, or customer service.

Data Rights

If you are in the [European Economic Area \(EEA\), Switzerland, or the UK](#), or a resident of [California](#) or

another U.S. state with an applicable privacy law, please refer to the respective dedicated sections below. Otherwise, at your request, and as required by applicable law, we will:

- Inform you of what personal data we have about you that is under our control;
- Amend or correct such personal data or any previous privacy preferences you selected, or direct you to applicable tools; and/or
- Delete such personal data or direct you to applicable tools.

In order to exercise any of your rights as to personal data controlled by Zoom, please click here. Where legally permitted, we may decline to process requests that are unreasonably repetitive or systematic, require disproportionate technical effort, or jeopardize the privacy of others. As an account owner or a user under a licensed account, you may also take steps to affect your personal data by visiting your account and modifying your personal data directly.

Children

Zoom does not allow children under the age of 16 to sign up for a Zoom account.

For educational organizations that use Zoom products and services to provide educational services to children under 18, Zoom's Children's Educational Privacy Statement is available here.

How to Contact Us

To exercise your rights, please click here. If you have any privacy-related questions or comments related to this Privacy Statement, please send an email to privacy@zoom.us.

You can also contact us by writing to the following address:

Zoom Video Communications, Inc.
Attention: Data Protection Officer
55 Almaden Blvd, Suite 600
San Jose, CA 95113

Or to our representative in the EU or UK:

Lionheart Squared Ltd
Attn: Data Privacy
2 Pembroke House
Upper Pembroke Street 28-32
Dublin
DO2 EK84
Republic of Ireland
email: zoom@LionheartSquared.eu

Lionheart Squared Limited
Attn: Data Privacy
17 Glasshouse Studios
Fryern Court Road
Fordingbridge
Hampshire
SP6 1QX

United Kingdom
Contact: zoom@LionheartSquared.co.uk

You can contact our Data Protection Officer by sending an email to privacy@zoom.us.

Retention

We retain personal data for as long as required to engage in the uses described in this Privacy Statement, unless a longer retention period is required by applicable law.

The criteria used to determine our retention periods include the following:

- The length of time we have an ongoing relationship with you and provide Zoom products and services to you (for example, for as long as you have an account with us or keep using our products);
- Whether account owners modify or their users delete information through their accounts;
- Whether we have a legal obligation to keep the data (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them); or
- Whether retention is advisable in light of our legal position (such as in regard to the enforcement of our agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation).

European Data Protection Specific Information

Data Subjects Rights

If you are in the EEA, Switzerland, or the UK, your rights in relation to your personal data processed by us as a controller specifically include:

- **Right of access and/or portability:** You have the right to access any personal data that we hold about you and, in some circumstances, have that data provided to you so that you can provide or “port” that data to another provider;
- **Right of erasure:** In certain circumstances, you have the right to the erasure of personal data that we hold about you (for example, if it is no longer necessary for the purposes for which it was originally collected);
- **Right to object to processing:** In certain circumstances, you have the right to request that we stop processing your personal data and/or stop sending you marketing communications;
- **Right to rectification:** You have the right to require us to correct any inaccurate or incomplete personal data;
- **Right to restrict processing:** You have the right to request that we restrict processing of your personal data in certain circumstances (for example, where you believe that the personal data we hold about you is not accurate or lawfully held).

To exercise your rights, please [click here](#). If you have any other questions about our use of your personal data, please send a request at the contact details specified in the How to Contact Us section of this Privacy Statement. Please note that we may request you to provide us with additional information in order to confirm your identity and ensure that you are entitled to access the relevant personal data.

You also have the right to lodge a complaint to a data protection authority. For more information, please contact your local data protection authority.

Legal Basis for Processing Personal Data

We only use your information in a lawful, transparent, and fair manner. Depending on the specific personal data concerned and the factual context, when Zoom processes personal data as a controller for individuals in regions such as the EEA, Switzerland, and the UK, we rely on the following legal bases as applicable in your jurisdiction:

- **As necessary for our contract:** When we enter into a contract directly with you, we process your personal data on the basis of our contract in order to prepare and enter into the contract, as well as to perform and manage our contract (i.e., providing Zoom products and services, features and services to account owners, their users, and those they invite to join meetings and webinars hosted on their accounts, and manage our relationship and contract, including billing, compliance with contractual obligations, and related administration). If we do not process your personal data for these purposes, we may not be able to provide you with all products and services;
- **Consistent with specific revocable consents:** We rely on your prior consent in order to utilize cookies to engage advertising and analytics partners to deliver tailored advertising and analysis of our website usage. You have the right to withdraw your consent at any time by visiting our cookie management tool, available Cookies Settings;
- **As necessary to comply with our legal obligations:** We process your personal data to comply with the legal obligations to which we are subject for the purposes of compliance with EEA laws, regulations, codes of practice, guidelines, or rules applicable to us, and for responses to requests from, and other communications with, competent EEA public, governmental, judicial, or other regulatory authorities. This includes detecting, investigating, preventing, and stopping fraudulent, harmful, unauthorized, or illegal activity (“fraud and abuse detection”) and compliance with privacy laws;
- **To protect your vital interests or those of others :**We process certain personal data in order to protect vital interests for the purpose of detecting and preventing illicit activities that impact vital interests and public safety, including child sexual abuse material; and
- **As necessary for our (or others’) legitimate interests, unless those interests are overridden by your interests or fundamental rights and freedoms, which require protection of personal data:** We process your personal data based on such legitimate interests to (i) enter and perform the contract with the account owner and/or reseller providing you with the products and services (which includes billing, compliance with contractual obligations, and related administration and support); (ii) develop, test, and improve our products and services and troubleshoot products and services; (iii) ensure authentication, integrity, security, and safety of accounts, activity, and products and services, including detect and prevent malicious conduct and violations of our terms and policies, prevent or investigate bad or unsafe experiences, and address security threats; (iv) send marketing communications, advertising, and promotions related to the products and services; and (v) comply with non-EEA laws, regulations, codes of practice, guidelines, or rules applicable to us and respond to requests from, and other communications with, competent non-EEA public, governmental, judicial, or other regulatory authorities, as well as meet our corporate and social responsibility commitments, protect our rights and property and the ones of our customers, resolve disputes, and enforce agreements.

International Data Transfers

Zoom operates globally, which means personal data may be transferred, stored (for example, in a data center), and processed outside of the country or region where it was initially collected where Zoom or its service providers have customers or facilities – including in countries where meeting participants or account owners hosting meetings or webinars that you participate in or receiving messages that you send are based.

Therefore, by using Zoom products and services or providing personal data for any of the purposes stated above, you acknowledge that your personal data may be transferred to or stored in the United States where we are established, as well as in other countries outside of the EEA, Switzerland, and the UK. Such countries may have data protection rules that are different and less protective than those of your country.

We protect your personal data in accordance with this Privacy Statement wherever it is processed and take appropriate contractual or other steps to protect it under applicable laws. Where personal data of users in the EEA, Switzerland, or the UK is being transferred to a recipient located in a country outside the EEA, Switzerland, or the UK which has not been recognized as having an adequate level of data protection, we ensure that the transfer is governed by the European Commission's standard contractual clauses. Please contact us if you would like further information in that respect.

California & Other U.S. States Notice at Collection

Categories of Personal Information Zoom Receives: Zoom may collect, or process on behalf of our customers, the following categories of personal data, as described above, in the "What Personal Data Do We Receive?" section: identifiers (such as in Account Information, Profile and Participant Information, Contact Information, and Registration Information), financial account information (such as in Account Information); commercial information (such as in Account Information); internet or other electronic network activity information (such as Device Information, Usage Information Regarding Meetings, Webinars, Message, Collaborative Features, and the Website, and Limited Information from Zoom Email and Calendar Services); audio, electronic, and visual information (such as in Content and Context from Meetings, Webinars, Messaging, and Other Collaborative Features) education information such as from university customers; inferences we derive from the preceding or other information we collect; and sensitive personal information (such as certain categories in Account Information, Content and Context from Meetings, Webinars, Messaging, and Other Collaborative Features).

Sources: We receive information from sources as described in the "What Personal Data Do We Receive?" section, including: from you (including through your use of our products and services); from partners; from customers; and from publicly available sources. We collect education information from schools that use our services. Please see our Children's Educational Privacy Statement for more information.

Zoom's business and commercial purposes for use: Zoom uses personal data for the following business and commercial purposes: to provide Zoom Products and Services; for Product Research and Development; for Marketing and Promotions (Zoom does not use meeting, webinar, or messaging content, or any content generated or shared as part of other collaborative features for any marketing or promotions); Authentication, Integrity, Security, and Safety; to Communicate with You; and for Legal Reasons. For more information, please see "How We Share Personal Data?" Categories of third parties to whom we disclose Personal Information for business purposes are described in "How We Share Personal Data?"

Zoom may permit advertising and analytics services that are intended to deliver advertising to you and/or analyze your interactions, based on your interactions with our website or app which may constitute a "sale" or "sharing" of data for targeted advertising purposes under certain state privacy laws. See "California & Other U.S. State Privacy Rights" for more information regarding your right to opt-out.

Retention: Zoom retains personal data for as long as required to engage in the uses described in this Privacy Statement, unless a longer retention period is required by applicable law. Additional detail on

retention criteria can be found under Retention, above.

California & Other U.S. State Privacy Rights

Under some U.S. state laws, including the California Consumer Privacy Act of 2018 (as amended by the California Consumer Privacy Rights Act) (CCPA), residents may have a right to:

- **Access** the categories and specific pieces of personal data Zoom has collected, the categories of sources from which the personal data is collected, the business purpose(s) for collecting the personal data, and the categories of third parties with whom Zoom has shared personal data, and obtain the personal data in a portable and, to the extent technically feasible, readily usable format;
- **Delete** personal data under certain circumstances;
- **Correct** personal data under certain circumstances; and
- **Opt out of the “sale” of personal data or “sharing” of personal data for targeted advertising purposes.** We do not sell your personal data in the conventional sense. However, like many companies, we may use advertising and analytics services that are intended to analyze your interactions with our website or app, based on information obtained from cookies or other trackers, including for delivering advertising to you (such as interest-based, targeted, or cross-context behavioral advertising). You can get more information and opt out of the use of cookies and other trackers on our website and app by clicking the Cookies Settings/Your Privacy Choices link, also on our homepage, and setting your preferences. You will need to set your preferences from each device and each web browser from which you wish to opt out. This feature uses a cookie to remember your preference, so if you clear all cookies from your browser, you will need to re-select your preferred settings. California and Connecticut residents may also set the Global Privacy Control (GPC) to opt out of the “sale” or “sharing” of your personal information for targeted advertising for each participating browser system that you use. Zoom does not have actual knowledge that it “sells” or “shares” the personal information of consumers under 16 years of age.
- **Appeal** a denial of your request. Some states provide additional rights to their residents. If we decline to process your request, you may have the right to appeal our decision. You can do so by replying directly to our denial or emailing privacy@zoom.us.

Zoom will not discriminate against you for exercising any of these rights, which is further in line with your rights under state law.

Sensitive Information. Zoom receives information that may be considered sensitive under some state laws, such as certain Account Information (e.g., financial information, log-in information), certain Content and Context from Meetings, Webinars, Messaging, and Other Collaborative Features and certain Limited Information from Zoom Email and Calendar Services (e.g., messaging content in cases described herein). Zoom processes sensitive personal information to provide Zoom products and services, for product research and development, for authentication, integrity, security, and safety reasons, to communicate with you, for legal reasons, and with your consent. Zoom does not use or disclose sensitive personal information (as defined under CCPA) for purposes of inferring characteristics about a consumer, or in any way that would require Zoom to provide a right to limit under the CCPA. Under certain laws, residents may also be permitted to opt out of certain profiling relating to automated processing analyzing certain categories of an individual’s information that would produce a legal or similarly significant effect. Zoom does not engage in this type of profiling of individuals.

To exercise your rights, please [click here](#) or call +1-888-799-0566. To opt out of the use of cookies on our sites for interest-based advertising purposes, follow the instructions above.

We will acknowledge receipt of your request within 10 business days, and provide a substantive response within 45 calendar days, or inform you of the reason and extension period (up to a total of 90 days) in writing.

These rights are not absolute, are subject to exceptions and limitations, and may not be afforded to residents of all states. In certain cases, we may decline requests to exercise these rights where permitted by law. We will need to verify your identity to process your access, deletion, and correction requests and reserve the right to confirm your state residency. To verify your identity, we may require you to log into your existing Zoom account (if applicable), give a declaration as to your identity under penalty of perjury, and/or provide additional information, such as providing at least two pieces of personal information relating to your account (which will be compared to information we have, such as profile information) or as we otherwise may already have in our possession, such as your email address and phone number. We will verify your consumer request by comparing the information you provide to information already in our possession, and take additional steps to minimize the risk of fraud. You may designate an authorized agent to submit your verified consumer request by providing written permission and verifying your identity, or through proof of power of attorney.

To see our Disclosure of Privacy Rights Requests, please [click here](#).

California's Shine the Light Law

California Civil Code Section 1798.83, also known as "Shine The Light" law, permits California residents to annually request information regarding the disclosure of your Personal Information (if any) to third parties for the third parties' direct marketing purposes in the preceding calendar year. We do not share Personal Information with third parties for the third parties' direct marketing purposes.

Changes to This Privacy Statement

We may update this Privacy Statement periodically to account for changes in our collection and/or processing of personal data, and will post the updated Privacy Statement on our website, with a "Last Updated" date at the top. If we make material changes to this Privacy Statement, we will notify you and provide you an opportunity to review before you choose to continue using our products and services.

[About](#)

[Zoom Blog](#)

[Customers](#)

[Our Team](#)

[Careers](#)

[Integrations](#)

[Partners](#)

[Investors](#)

[Press](#)



Order Form Number: Q2304420
Valid Until: 10/29/2023

Zoom Video Communications Inc. ('Zoom')
55 Almaden Blvd, 6th Floor
San Jose, CA

Billed To Customer: Citrus County Schools Account Legal Name: CITRUS COUNTY SCHOOL BOARD Contact Name: Kathy Androski 1007 W Main St Inverness, Florida 34450, United States Email Address: androskik@citruschools.org Phone: 352-726-1931	Sold To Customer: Citrus County Schools Account Legal Name: CITRUS COUNTY SCHOOL BOARD Contact Name: Kathy Androski 1007 W Main St Inverness, Florida 34450, United States Email Address: androskik@citruschools.org Phone: 352-726-1931
Auto Renew: No Initial Paid Subscription Term: 12 Month Paid Period Start Date: 09/29/2023	Billing Method: Email Currency: USD Payment Term: Net 30

This Zoom Order Form and any other Order Forms that reference this Order Form are governed by the Zoom Terms of Service found at <https://explore.zoom.us/en/terms/> (unless Customer and Zoom have entered a written governing Master Subscription Agreement, in which case such written agreement will govern).

SERVICE	BILLING PERIOD	QUANTITY	PRICE	TOTAL
Education Annual	Annual	1290	USD 28.78	USD 37,125.00
Webinar 500 Annual	Annual	5	USD 690.00	USD 3,450.00

(Before Taxes)	
Annual Payment:	USD 40,575.00

Payment Schedule Summary (Before Taxes)
First Payment: USD 40,575.00

Other Terms & Notes

Named Host - means any subscribed host who may host an unlimited number of meetings during the Term using the Service. Any meeting will have at least one Named Host. Unless Customer has purchased an extended capacity, the number of participants (participants do not require a subscription) will not exceed 300 per meeting. Named Host subscription may not be shared or used by anyone other than the individual to whom the Named Host subscription is assigned.

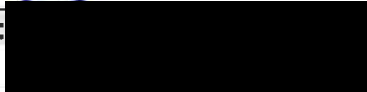
Zoom EDU subscriptions are intended for student and faculty and pedagogical interaction within a classroom environment, or the administration thereof and may not be used for any commercial purpose. Zoom EDU subscriptions may not be purchased by hospitals, medical centers, clinics, or other affiliated organizations not specifically involving student and faculty and pedagogical interactions within a classroom environment or the administration thereof.

Fees - The fees for the Services, if any, are described in the Order Form. The actual fees may also include overage amounts or per use charges for audio and/or cloud recording in addition to the fees in the Order, if such use is higher than the amounts described in the Order, and you agree to pay these amounts or charges if you incur them. Invoicing for Services begins on the first day that the service is available for use by the Customer and monthly thereafter for the duration Term, except for annual pre-pay option which is invoiced once in the first month of the annual term. Amendment orders will co-term with the existing subscription term end date. Invoices are pro-rated from paid period start date to base subscription end date. Purchase order, if any, issued in connection with this order should reference the above order form number. Commitments not utilized by the Customer during the month for which they are committed may not be carried forward into any subsequent month or term.

All prices shown for Zoom and Zoom Phone services are exclusive of taxes. The term 'taxes' referred herein should encompass: US state and local taxes, VAT, GST, HST (or any other consumption taxes), Digital Service Taxes and Withholding Taxes that may apply upon making payments to Zoom.

Professional Services, if purchased, will be presented in a separate Order Form.

Accepted and agreed as of the date specified below by the authorized representative of Customer

Signature:	
Print Name:	Douglas A. Dodd
Date:	10/10/2023
Zoom Service Effective Date:	09/29/2023
PO # (If Applicable):	
VAT # (If Applicable):	
TAN # (If Applicable):	
CIN # (If Applicable):	

The Services will be activated within 48 hours of order signature or Zoom Service Effective Date, whichever is later.

Zoom reserves the right at its sole discretion to accept Order Forms received after the Valid Until date.

If a PO# is required for processing the invoice related to this order, please provide a PO with this order. If issuance of PO is delayed, please provide a PO within 5 days of the service effective date via email to purchase-orders@zoomus.zendesk.com. Notwithstanding the foregoing, the

period for payment shall commence as of the applicable invoice date. Such payment period shall not restart based on any delays in issuing a Purchase Order or any procurement process.

