STANDARD STUDENT DATA PRIVACY AGREEMENT

OH-NDPA-V1

AGREEMENT TYPE

Hudson City Schools

LEA

and

Uptale

Provider

3-13-2024

Date

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between:
[Hudson City Schools], located at [76 N. Hayden Pkwy, H] (the "**Local Education Agency**" or "**LEA**") and [Uptale], located at [128 rue de la Boétie 75] (the "**Provider**").
WHEREAS, the Provider is providing educational or digital services to LEA.
WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and
WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

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

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

2. **Special Provisions.** ***Check if Required***

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

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

   ☑ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

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

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

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

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

The designated representative for the LEA for this DPA is:

Name: Stephanie Swiderski Title: Technology Coordinator

Address: 76 N. Hayden Pkwy, Hudson, OH

Phone: 330-653-1360 Email: swiderss@hudson.k12.oh.us

The designated representative for the Provider for this DPA is:

Name: Martin Sebban Title: Sales and Partnership Ma

Address: 128 rue de la Boétie 75008 Paris

Phone: 33(0)680 77 76 99 Email: martin@uptale.io

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

LEA [Hudson City Schools]

By: Stephanie Swiderski Date: 3-13-2024

Printed Name: Stephanie Swiderski Title/Position: Technology Coordinato

Provider [Uptale]

By: Ristagno David Digitally signed by Ristagno David Date: 2024.03.13 15:44:07 +01'00' Date: 3-13-2024

Printed Name: David Ristagno Title/Position: CEO

STANDARD CLAUSES
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

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

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

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

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

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

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

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

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

ARTICLE III: DUTIES OF LEA

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

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

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

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

ARTICLE IV: DUTIES OF PROVIDER

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

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

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

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

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

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

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

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the 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 services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit 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 the Provider and as it becomes available:

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

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

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

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

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

ARTICLE VI: GENERAL OFFER OF TERMS

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

ARTICLE VII: MISCELLANEOUS

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

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

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

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

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

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

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

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

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

EXHIBIT "A"
DESCRIPTION OF SERVICES

Education License: complete control to create, oversee, and launch your immersive experiences independently.

Unrestricted access to our comprehensive online academy.

Online training and personalized coaching services might be included.

Dedicated online support is included at support@uptale.io.

EXHIBIT "B"
SCHEDULE OF DATA

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

Category of Data	Elements	Check if Used by Your System
	Phone	☐
Parent/Guardian ID	Parent ID number (created to link parents to students)	☐
Parent/Guardian Name	First and/or Last	☐
Schedule	Student scheduled courses	☐
	Teacher names	☐
Special Indicator	English language learner information	☐
	Low income status	☐
	Medical alerts/ health data	☐
	Student disability information	☐
	Specialized education services (IEP or 504)	☐
	Living situations (homeless/foster care)	☐
	Other indicator information-Please specify:	☐
Student Contact Information	Address	☐
	Email	✔
	Phone	☐
Student Identifiers	Local (School district) ID number	✔
	State ID number	☐
	Provider/App assigned student ID number	✔
	Student app username	✔
	Student app passwords	✔
Student Name	First and/or Last	✔
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	☐
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	☐
Student Survey Responses	Student responses to surveys or questionnaires	☐
Student work	Student generated content; writing, pictures, etc.	✔
	Other student work data -Please specify:	☐
Transcript	Student course grades	☐
	Student course data	☐

Category of Data	Elements	Check if Used by Your System
	Student course grades/ performance scores	☐
	Other transcript data - Please specify:	☐
Transportation	Student bus assignment	☐
	Student pick up and/or drop off location	☐
	Student bus card ID number	☐
	Other transportation data – Please specify:	☐
Other	Please list each additional data element used, stored, or collected by your application: Immersive Learning Experiences based on media files and metadata input by a creator user Usage data of the platform Devices registered on the platform	✔
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

EXHIBIT "C"
DEFINITIONS

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

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

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

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

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

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

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

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

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to,

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

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

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

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

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[**Insert LEA Name**] _____Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[**Insert categories of data here**]_____

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

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

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

[**Insert or attach special instructions**]_____

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By [**Insert Date**]_____

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Company Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. **Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and [Hudson City Schools] ("Originating LEA") which is dated [3-13-2024], to any other LEA ("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, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: david@uptale.io.

[Uptale]

BY: Ristagno David Digitally signed by Ristagno David Date: 2024.03.13 15:45:02 +01'00' Date: 3-13-2024

Printed Name: David Ristagno Title/Position: CEO

2. **Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the [Hudson City Schools] and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

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 Cybersecurity Framework Version 1.1
☐	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
☐	International Standards Organization	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 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 [State]

Version _____

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

[THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK]

EXHIBIT "H"

Additional Terms or Modifications

Version 1_____

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

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

As an exception to Article V.3 and Exhibit F, the security measures implemented by the Provider for the Services as described in Exhibit A are detailed in the security document provided by the Provider (Exhibit I). The Provider has also taken steps towards ISO27001 certification which is an ongoing project

Exhibit I

Uptale Security Reference

Contents

General Description

Uptale is a SaaS platform hosted in Microsoft Azure Cloud enabling users to build, host, publish and consume interactive Immersive Learning experiences in Virtual Reality and 360°. Created experiences are securely hosted on the Uptale platform, are delivered through the web, and can be played by a web browser using WebVR technology (HTML5 and CSS) or a dedicated Player Application using Unity. The experiences can be consumed through any device (desktop, laptop, smartphone, VR Headsets/HMDs,…) from the cloud platform or a LMS (like a standard e-learning piece of content). Advanced Data dashboards are also available through the same platform and provide data reports for content creators, trainers and learners.

Uptale can also be integrated to corporate systems through different means while guaranteeing security.

Here are the key components of Uptale:

- Web application for the creator platform interface, the WebVR experience, the data dashboards, user management and resource center
- No-SQL Storage for storing Experience manifests and media files
- Video and Audio online encoding platform
- Data pipe
- Private APIs for some advanced features like speech recognition

The front-end web application is using HTML5 and javascript and does not require any plugin (like Flash, Silverlight, Java, ActiveX,…), is compatible with most of modern browsers, and works on mobile.

No app installation is required, however for better performance, immersion in VR and offline use we recommend to use:

- The Uptale Player App for Android, iOS, Lenovo Mirage VR S3, Pico G2 4K, Oculus Quest (1, 2 and Quest Pro), HTC Vive Focus, Oculus Go and Windows, which provides both a smoother experience and offline options.

The Windows version of the app is compatible with all major Head Mounted Headsets if SteamVR is running on the computer : HTC Vive, Oculus Rift, Windows Mixed Reality.

Our service is hosted on Microsoft Azure Cloud, mostly using Azure Services providing geo-redundancy, fault-tolerance mechanism, and good SLA. More information about Azure Security here : https://www.microsoft.com/en-us/trustcenter/security/azure-security

https://azure.microsoft.com/en-us/blog/microsoft-azure-leads-the-industry-in-iso-certifications/

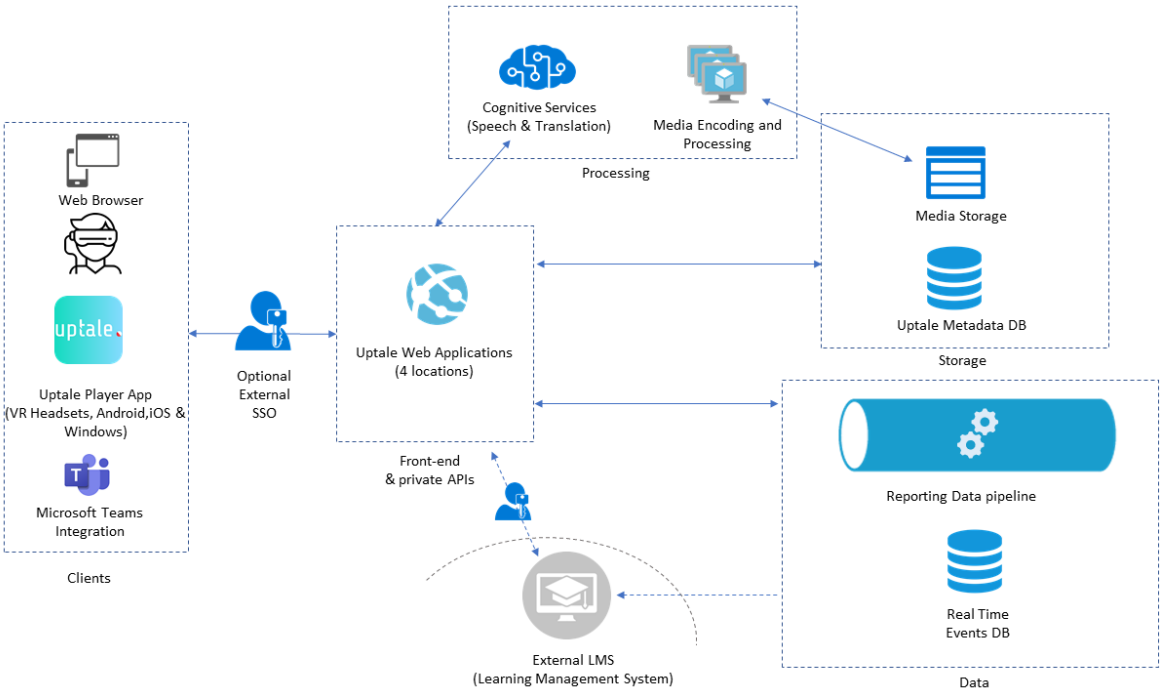
Several Azure regions are used:

- Data hosting: France, West Europe (Netherlands) and North Europe (Ireland)

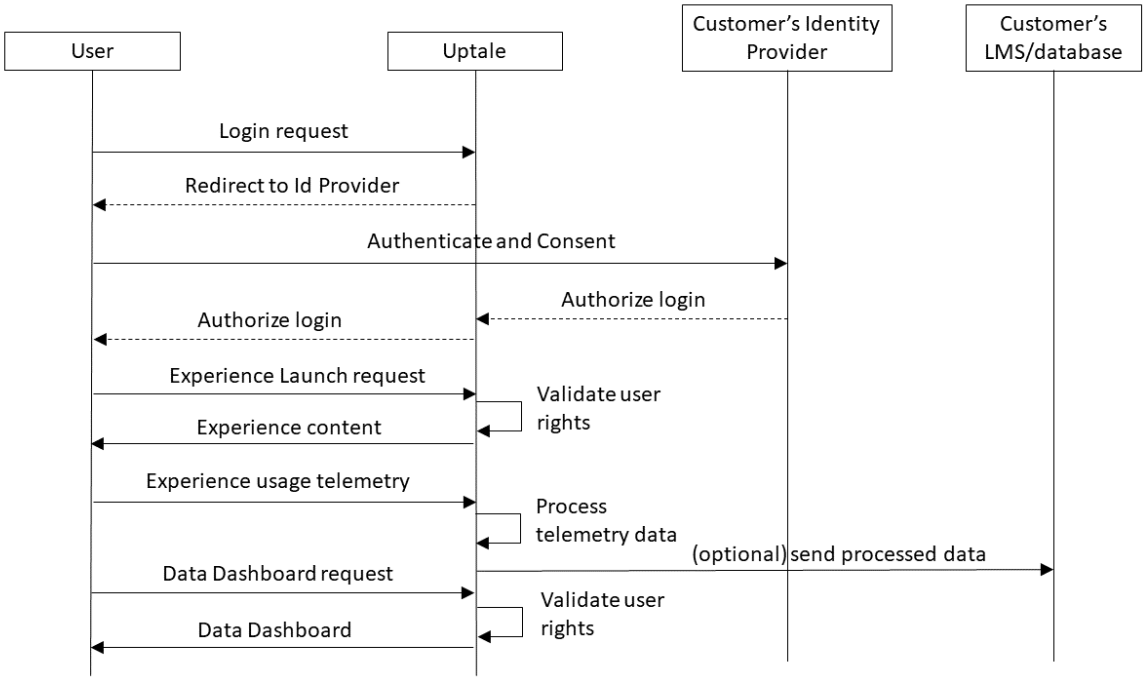
- Stateless web servers for better performances: West Europe (Netherlands), Southeast Asia (Singapore), Central US, Brazil South and Australia

Uptale is built on a multi-tenant architecture, based primarily on scalable services from Azure. Scaling the platform by adding additional instances can happen easily.

Here's a summary of the functional architecture of the service:



One of the main complete scenarios for a user on the platform would be to login, then launch an Uptale private Experience, and then review the data of the experience.
A high level sequence diagram, with SSO and LMS integration, could be the following (the SSO part has been simplified, it would follow the OAuth or SAML protocols depending on the one implemented):



Data Protection

Collected data are Basic personal data and are located in the EU (France and West Europe Azure region, in Netherlands, and replicated to North Europe in Ireland) and accessed through the users' account, and in some cases by Support/Administrators with the agreement of the customer.

Regarding users' training sessions on Uptale, as well as the activity of the content creators on the authoring tool, these data are mainly collected in order to produce data report pages that are available to users on the platform. These pages are secured through access control depending on user's rights in the system.

If these data end up being used for any other mean (like a general case study for instance), they would be aggregated and entirely anonymized. Customers can ask for permanent deletion of their data at any time.

Despite all our security measures, in the event of a detected data breach, we have an internal procedure which basically consists of 4 steps:

- Contain it by all means, if necessary, by cutting off access to the platform
- Determine the risks caused by this violation
- Depending on the severity, contact the customer
- Track the incident and Analyze the origin

Subcontractors

Uptale may use subcontractors to :

- Develop the platform. In this case, developer vendors never have access to the Production environment, have signed a confidentiality clause with Uptale and the entire source code is reviewed by the Uptale Development team (Full-time employees) before reaching Production environment.
- Produce and Deliver VR Experiences through the Uptale Platform for the Customer. This does not require any specific access to any development or production environment. Vendor would have signed a confidentiality clause with Uptale and would work in a separate and isolated workspace. The experience will be sent to the customer's workspace when it is done.

Physical Access Surveillance and Control

Physical access surveillance and control to the premises hosting the service and data are guaranteed by Microsoft Azure : https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Availability

A full backup of all data (including metadata, media files, user management data, usage data) is automatically performed every 24 hours. Backup media are not physically managed by Uptale and are protected by the security and high availability infrastructure of the Microsoft Azure cloud. Cloud Services are used to back up the data and store it on a separate instance, still in Europe, and using the same level of security as the production platform.

Recovery Time Objective (RTO): 48 hours

Recovery Point Objective (RPO): 24 hours

Most Data storages are geo-redundant (replicated to North Europe Region, in Ireland).

A CDN option is available (called "Distributed"), in this case, medias may be cached on Akamai worldwide network, and better performances may be observed. (Not enabled by default)

Scheduled and Unscheduled maintenance operations happen approximately once every 2 months (usually for data migrations or upgrades required by our cloud provider). Most of them are seamless.

Seamless upgrades of the platform are very frequent and may happen several times a week to provide continuous improvements to our users.

Our Standard SLA is 99%.

In case of issue accessing the services, a ticket can be opened by emailing support@uptale.io.

Security standards and Protocols

Uptale supports Single Sign On (SSO) integration using the OAuth 2.0, SAML2 and Open ID Connect standards, other types of SSO protocols can be implemented if required.

Such an integration requires a bit of development and configuration effort depending on the level of integration and chosen protocol: exchange of certificates, configuration of callback urls, testing phase, advanced integrations such as role mapping, ...

All data between Uptale servers and Client applications are securely encrypted and using TLS 1.2 or above.

HTTPS protocol on the standard port is enforced (HTTP is blocked), as well as TLS 1.2 (or above) and all the traffic is encrypted with a valid Sha256 SSL certificate.

The certificate complies with Certificate Transparency Standard (https://www.certificate-transparency.org)

Important cookies are marked as secure in order to avoid cookie and session theft

All passwords are hashed using a SHA-512 algorithm within the database, none is stored in clear

We have a configurable password composition rule system with the following rules available (Not applicable with an SSO integration):

- Minimum password length

- Minimum number of capital letters

- Minimum number of lowercase letters

- Minimum number of special characters

- Minimum number of digits

- Minimum number of different character categories between upper case, lower case, special characters and numbers

- Maximum age of the password before change

- Non reuse of previous passwords

All data at rest are encrypted using Azure Storage, Azure Cosmos DB, and Azure SQL's encryption systems:

- https://docs.microsoft.com/en-us/azure/cosmos-db/database-encryption-at-rest
- https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
- https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-azure-sql

Source Code and Operations Excellence

Uptale pays particular attention to the excellence of the implemented code as well as its security.

- Source code is stored in a secured source control system with versioning capabilities: Git on Azure DevOps.
- Principle of least privilege is applied in regard to source code and deployment environments.
- Passwords and other secrets are never stored in code. Azure Key Vault is leveraged to store and access secrets.
- Code review approvals are mandatory before any pull request in the source control system's main branches
- Code quality, style and readability is enforced during the code review process: indents, comments, proper Exception and Error management, instrumentation/logging, recommended design patterns, …
- Modern and Trusted Managed Cloud Services are preferred when applicable to guarantee constant security updates and more effective scalability, elasticity, availability, security and audit capabilities. i.e : Azure App Services, Azure CosmosDB, …
- All Bugs, Development Tasks/Stories/Features, as well as Incidents, are stored and accessed through a secured work item management system in Azure DevOps
- Most deployments to all environments (Dev, Production, Shadow Prod, Custom,…) are entirely automated, with very effective rollback mechanisms, sometimes automated when failure is detected during deployment.
- Automated alerts are in place when failures or availability drops are detected
- Administrator accesses to Production are logged and cannot be modified
- Performance and Service Health real time dashboards are available and monitored after each Deployment to Production
- A static code analysis is run at each build
- A dynamic code analysis is run on a regular basis

Continuous Information System Security Improvement Process

The development and operation team follow a 12-week sprint cadence of planning. Deployments happen much more frequently, up to several times a week.

Before each of these sprints, the team:

- Ensures that Security Stories are part of the sprint
- Review the access rights of the administrators of the platform and the production environment. Ensure the principle of least privilege is followed.
- New security stories are considered and added to the backlog
- Communicates to the rest of the company the potential relevant new security measures and policies

Additionally and continuously:

- Critical updates of packages, especially the ones containing security patches are being applied
- Code reviews with approval of a senior developer are mandatory prior any code check in
- Security & Privacy trainings are being delivered to all employees on an annual basis.

All detected vulnerabilities are being tracked and added to the story backlog and treated with high priority

Installation Security

Most of Uptale services are running on managed Cloud services of Microsoft Azure, the underlying physical and logical machines are managed by the cloud infrastructure. Both Security patches and malware protection are ensured by Microsoft.

Besides these Managed Services, a few Stateless Virtual Machines are required to run some Workers. For those VMs:

- Antivirus is running with regular update of signatures
- Security updates are managed by the Azure VM Update Management feature. The technical team receives alerts when a security patch is available, and such Updates are being applied quickly, other types of Updates are done regularly. https://docs.microsoft.com/en-us/azure/automation/automation-tutorial-update-management

Business Continuity

Service availability

The high availability of the service is guaranteed by several architecture implementations:

- Front-end Web instances are situated in various locations around the world
- Traffic is load balanced among these instances using a Distributed Traffic Manager
- Metadata storage is done on a No-SQL Cloud-Managed solution, guaranteeing a high availability (99.99%) and easily scalable in terms of number of instances.
- Media storage (for media content such as 360° videos/pictures, sounds, 3D objects,…) is geo-replicated between 2 different locations (North Europe and West Europe)

- Internal Search Engine has 2 replicas, providing a high availability for search queries (99.9%)
- Several services are entirely managed by the cloud and can provide high availability and elasticity by default (cognitive services, analytics services, serverless functions, …)

Continuity Plan

The Uptale platform is entirely hosted on Microsoft Azure Cloud. Information about the Azure Cloud availability and disaster management can be found here: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability

Extract:

"The Microsoft Cloud Infrastructure and Operations team designs, builds, operates, and improves the security of the cloud infrastructure. This team ensures that the Azure infrastructure is delivering high availability and reliability, high efficiency, and smart scalability. The team provides a more secure, private, and trusted cloud.

Uninterruptible power supplies and vast banks of batteries ensure that electricity remains continuous if a short-term power disruption occurs. Emergency generators provide backup power for extended outages and planned maintenance. If a natural disaster occurs, the datacenter can use onsite fuel reserves.

High-speed and robust fiber optic networks connect datacenters with other major hubs and internet users. Compute nodes host workloads closer to users to reduce latency, provide geo-redundancy, and increase overall service resiliency. A team of engineers works around the clock to ensure services are persistently available.

Microsoft ensures high availability through advanced monitoring and incident response, service support, and backup failover capability. Geographically distributed Microsoft operations centers operate 24/7/365. The Azure network is one of the largest in the world. The fiber optic and content distribution network connects datacenters and edge nodes to ensure high performance and reliability."

Access rights

Uptale has an advanced built-in Role Based Access Control (RBAC) mechanism in place to control user rights and guarantee the logical segregation between Environments and Workspaces.

Access to the platform and the Experiences is secured and access is granted or not depending on the user's rights and the Experience's configuration.

A user can have **Roles** in one or several **Workspaces**

A **Workspace** belongs to an **Environment**

Each user is attached to an **Environment.**

The main different Roles a user can have within a Workspace are :

- Workspace Administrator
- Creator
- Learner
- Trainer

A **Workspace** contains **Experiences** (Experience = Immersive learning module).

Experiences can only be Created and Modified by **Creator or Workspace admin** users belonging to the **Workspace** of the **Experience.**

An **Experience** can be marked as **Public** or **Private**.

A **Public** Experience can be Played by any type of user, even anonymous (someone not even logged in), accessing the right link of the Experience.

A **Private** Experience can only be Played by an authenticated user with rights on the same workspace (having one of the 4 Roles).

By **default**, Experiences are **Private**.

A **Workspace Admin** account is also an administrator of the users within the team.

A **Trainer** is an administrator of the Learners within a team. She cannot edit experiences or manage Creator/Workspace admin accounts.

There is a special Role, called "**Environment Administrator**", that is associated to an Environment instead of a Workspace. Such right grants the ability to manage Workspaces (create, rename, delete), and manage all Users and User Roles of the Environment.

Environment Administrator right is granted manually by the Uptale team.

Here is a summary of the rights of the different roles:

	Play	Edit	View Global Data	Go Public	Manage Workspace	Manage Users
Env Administrator	✓	✓	✓	✓	✓	✓
Workspace administrator	✓	✓	✓	✓	✗	✓
Trainer	✓	✗	✓	✗	✗	! Only Learners

Creator	✓	✓	✓	✗	✗	✗
Learner	✓	✗	✗	✗	✗	✗

Access to data by the Uptale team

The virtual DevOps team (5 persons at this time) has access to the Production servers in order to maintain it, and have technically the ability to access all of the data as stored on the server.

All of their access to the Production servers are secured by a Multi-Factor Authentication.

On the Uptale platform, by default, the Uptale team does not have access to Customer's experiences and data. However, there is a process in place to authorize the Uptale team to access to experiences and data of a given team (for support purposes for example).

Flow control and filtering

DDoS protection is enabled by default in Azure. More information here:

https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview

Traceability

When accessing or doing operations on the cloud infrastructure as an administrator, logs include very detailed information, including date, time, User ID, IP, and success of the operation. The detailed schema is here: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-schema

About tracking actions on the platform, logs are mostly functional, and their main purpose is reporting and analytics for the good use of the platform. These logs include date, time, UserID, and custom details depending on the actions.

Penetration testing

Penetration tests are conducted regularly on the platform by a third-party auditor specialized in security. All findings are analyzed, categorized and prioritized, then are planned for resolution or closure according to their priority.

Domains called by the client applications

- my.uptale.io
- <customername>.uptale.io (if SSO is in place)
- cdn.uptale.io
- auth.uptale.io
- uptalestore.blob.core.windows.net
- westeurope.api.cognitive.microsoft.com
- dc.applicationinsights.microsoft.com
- dc.applicationinsights.azure.com
- dc.services.visualstudio.com
- westeurope-0.in.applicationinsights.azure.com