DATA PROCESSING AGREEMENT

THE PARTIES:

1. **TUDesc B.V.**, with a registered office at 2628CE, Delft, Landbergstraat 15, The Netherlands, represented by Dr A.H.W. van der Zanden, who, as Chief Executive Officer is authorised to sign this agreement,

hereinafter referred to as: "**the Processor**", and

2. **University Institute**, with a registered office at **postal code, city, address**, hereby represented by **Name, Affiliation** ("**the Controller**")

1 and 2 referred to individually as: "**the Party**" and jointly: "**the Parties**"

Whereas:

On **Date**, the Parties entered into a contract concerning **Mutual Confidence and Shared Responsibilities**. In the implementation of this contract, personal data and configuration data for education spaces in software application "Interactive Education Spaces Configurator" or one of its sub-modules will be processed by the Processor on behalf of the Controller.

The Controller is committed to the protection of these personal data and configuration data. For this reason, the Parties are using this Data Processing Agreement (Article 28, paragraph 3 of the General Data Protection Regulation, GDPR) and the associated appendices, i.e.:
- Overview of processing of personal data and purposes of processing (Appendix A);
- Overview of processing by sub-processor (Appendix B);
- Overview of security measures (Appendix C);
- Incident management (Appendix D).

HEREBY AGREE AS FOLLOWS:

1. General

a. Terms used in this Data Processing Agreement have the same meaning as in the General Data Protection Regulation (Regulation (EU) No. 2016/679).
b. In the event of any conflict between this Data Processing Agreement and the Contract, the Terms and Conditions of TUDesc, available at https://tudesc.com/terms will take precedence.
c. This Data Processing Agreement is subject to Dutch law. Disputes concerning this Data Processing Agreement will be put to the Court in The Hague, The Hague location.

2. Data processing – and general obligations

a. All personal data will be regarded as confidential data and treated as such. The Processor is permitted to use the personal data solely for the purposes of implementing the Contract and solely on the instructions of and on behalf of the Controller. An overview of all permitted processing has been included in Appendix A.
b. The Processor will refrain from using the personal data for its own purposes, for the advantage of or on behalf of third parties or for any other purposes, unless a statutory obligation under applicable law obliges it to do so, in which case the Processor will notify the Controller of that

statutory obligation prior to processing, unless applicable law prohibits any such announcement for compelling reasons of general interest.

c. The Parties will comply with applicable privacy legislation and provide each other back and forth with all necessary cooperation and information in order to meet their statutory duties.

d. The Controller retains intellectual and property rights pertaining the personal data.

e. If, contrary to that stipulated in this Data Processing Agreement and/or the GDPR and/or other applicable legislation and regulations concerning the processing of personal data, the Processor determines the purposes and means for processing the personal data, the Processor will be deemed to be the Controller for said processing.

3. Confidentiality

The Processor will only reveal personal data to staff members for whom knowledge of the personal data is strictly necessary for the purpose of implementing the Contract, except in cases where other statutory obligations apply to them. The Processor will also guarantee that authorised staff members are bound by a duty of confidentiality and abide by the provisions of this Data Processing Agreement.

4. Security

a. Pursuant to Articles 28 and 32 of the GDPR, the Processor will take appropriate technical and organisational measures to guarantee a level of security in accordance with the risk. The Processor will ensure that these measures take account of current technology, the cost of implementation, the nature, scope, context and purposes of processing and the risks of varying likelihood and severity for the rights and freedoms of data subject(s). Consideration will also be given to risks that may result from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to data transmitted, stored or otherwise processed.

b. The Processor follows the security policy and have taken measures as described in Appendix C. Since security risks are continually changing, the Processor will regularly update and improve the security measures.

5. Data Protection Impact Assessment

According to the TU Delft Data Protection Impact Assessment (DPIA) checklist the software application “Interactive Education Spaces Configurator” have low risk for the personal data and configuration data. In case the Controller is obliged to conduct a Data Protection Impact Assessment (DPIA) the Processor will notify the Controller about the following:

i. a description of the processing envisaged;

ii. an assessment of the risks to the rights and freedoms of data subjects in view of the nature, scope, context and purposes of the processing;

iii. the measures intended to address the risks stated under (ii), including safeguards, safety measures and mechanisms to ensure the protection of the personal data and demonstrate compliance with the GDPR, taking account of rights and legitimate interests of the data subject(s) and persons concerned.

6. Sub-processor

a. The Processor refrains from outsourcing the processing of personal data under this Data Processing Agreement to sub-processors without prior permission from the Controller. The Controller grants permission for the use of sub-processors only in the event that this has been included in Appendix B. In the event of any intended change (addition or replacement) to one

or more sub-processors during this Agreement, the Processor provides the Controller with notice of this change.

b. In the event that the Processor outsources its obligations under this Data Processing Agreement with permission from the Controller, the Processor must enter into a sub-processing agreement that imposes the same conditions and obligations on the sub-processor as those imposed on the Processor in this Data Processing Agreement. If the sub-Processor fails to meet its obligations towards the Processor, the Processor will take action to the best of their knowledge to be compliant with the data processing agreement.

c. Dutch law will apply to the provisions concerning the outsourcing of this Data Processing Agreement.

d. The sub-processor maintains a list of the sub-processing agreements entered into as part of this Data Processing agreement. This list will be updated at least once annually.

e. Only with prior written permission from the Controller the Processor is allowed to process or arrange the processing of personal data in countries outside the European Economic Area (EEA) or provide personal data to organisations outside the EEA.

7. Requests from data subjects, government and supervisory authorities

a. Requests from data subjects

Processor will cooperate fully in enabling the Controller to comply with the requests of data subjects, for example by providing data subjects with access to the personal data of relevance to them, removing, supplementing, transferring, protecting and rectifying personal data and providing evidence that the request has been met.

b. Requests from government and supervisory authorities

In close consultation with the Controller, the Processor will cooperate fully in any investigations conducted or requests made by government and supervisory authorities concerning the Controller and will provide all information of relevance to this. If the Processor receives a request of this kind addressed to it, it will immediately notify the Controller and the Parties will consult on the steps to be taken, unless that is prohibited in view of the nature of the request.

c. In order to safeguard the protection of personal data, the Processor will in that case ensure that it does not provide the government or supervisory authority with more personal data than is strictly necessary in order to meet the public body’s request.

8. Audit

a. Due to the low-risks, the Processor has no obligation to have an independent external expert conduct an audit every once in a while as long as the Processor is compliant with the Contract, the Data Processing Agreement, the GDPR and other applicable legislation and regulations concerning the processing of personal data.

b. The Controller is entitled to have an audit of the Processor's organisation conducted by an independent external expert in order to demonstrate that the Processor is compliant with the Data Processing Agreement, the GDPR and other applicable legislation and regulations concerning the processing of personal data. The Controller can make use of its right to have an audit of the Processor conducted at its request a maximum of once annually or more frequently in the event of a specific suspicion that the Processor is not complying with the Data Processing Agreement and/or the GDPR and/or other applicable legislation and regulations concerning the processing of personal data.

c. The Controller provides the Processor with notice of the audit at least 14 (fourteen) days in advance of it. The audit may not cause unreasonable disruption to the Processor's normal business activities.
d. Costs of the audit conducted at the request of Controller shall be paid by the Controller.
e. If it is determined during an audit that the Processor is not complying with the Data Processing Agreement, and/or the GDPR and/or other applicable legislation and regulations concerning the processing of personal data, the Processor immediately takes all measures reasonably necessary to ensure that the Processor is compliant.

9. Reporting of data breaches

a. The Processor will have procedures in place aimed at ensuring the reasonable detection of security incidents and data breaches and taking action in response, including remedial measures.
b. In order to enable the Controller to fulfil its notification obligations, the Processor notifies the Controller of any breach of security within 24 hours. Reports include:
    i. the nature of the breach and, where possible, the categories of data subjects and personal data records concerned and the approximate number of data subjects and personal data records concerned;
    ii. the name and contact details of the Processor's data protection officer or another point of contact where further information can be obtained concerning the breach;
    iii. the likely consequences of the personal data breach;
    iv. the measures for addressing the personal data breach, including, where appropriate, the measures to mitigate its possible adverse effects.
c. With regard to every breach as referred to under 9a, the Processor will ensure that it provides the Controller with all cooperation that might reasonably be expected from the Processor, including the provision of sufficient information and support relating to investigations by the supervisory authority:
    i. in order to rectify and investigate the breach and prevent future breaches;
    ii. in order to limit the impact of the breach on the privacy of data subjects; and/or
    iii. in order to limit the damage incurred by the Controller as a result of the breach.
d. The Processor documents any personal data breaches, including the facts concerning the personal data breach, the consequences of it and any remedial measures taken. The Processor provides this documentation to the Controller as soon as it is requested following the format as is presented in Appendix D.
e. Unless legally required to do so, the Processor will not notify the supervisory authority and/or data subjects of a security breach without prior written permission from the Controller.

10. Retention periods

a. The Processor will not retain the personal data for longer than is strictly necessary but at least fifteen months after the TUDesc License of Use or Sub-license has ended.
b. Where necessary and possible, the Processor follows the retention instructions given by the Controller.

11. Liability and indemnity

a. The TUDesc application, its sub-modules, its generated figures and pictures, its dashboard information, and its API functionalities are reliable and accurate to the best of the knowledge

of the Processor. Any liability arising out of or deriving from the Product towards third parties is explicitly excluded. The Terms & Conditions are available at https://tudesc.com/terms.

b. TUDesc is not liable for indirect, incidental or consequential damage of whatever nature suffered by the Controller. In the event of any direct damage for which TUDesc is legally liable to the Controller, the liability will be limited to items that fall under the cover of its professional liability insurance, whereby any liability is furthermore limited to the amount paid out under this insurance policy.

12. Change

a. In the event of an intended change to the processing of personal data, such as the deployment of a new sub-processor, a change in the transfer of personal data to third countries and/or international organisations or changes to the security measures taken, the Processor is obliged to notify the Controller about the intended changes and the Parties will consult as soon as possible on the consequences for this Data Processing Agreement.

b. In the event of any change to the current policy rules of the supervisory authority, the Parties will make use of Appendix C to implement the changes required in order to comply with the new policy rules.

13. Duration and termination

a. The duration of the Data Processing Agreement is identical to that of the Contract. It cannot be terminated prematurely or separately from the Contract.

b. The Parties agree that, within fifteen months of the termination of the Data Processing Agreement, the Processor destroys, return and/or transfer all personal data and copies it has processed, some of which may be held by persons/legal persons deployed by the Processor, including but not limited to staff members and/or sub-processors, and provides written confirmation of this to the Controller, unless the law prohibits return or destruction. In the latter event, the Processor guarantees that it will observe confidentiality with regard to the personal data processed and will no longer actively process the personal data.

c. When this Data Processing Agreement terminates, the provisions that are intended to continue to apply after it will remain in force, such as Article 2.d (ownership) and Article 3 (confidentiality).

AGREED AND SIGNED:

University of …	TUDesc B.V.
Name:	Name:
Job title:	Job title:
Date:	Date:

Appendix A: Personal Data

Processing Description of the subject and duration of the processing	**Purposes** Description of the nature and objective of the processing	**Categories** Description of the categories of data subjects	**Personal data** Description of the type of personal data being processed	**License data** Description of type of license data being processed
Registered Staff in the TUDesc application during the License of Use period up to a maximum extension of 15 months after the License of Use has ended.	*Storing of users, roles, rights, and permissions, i.e. to enable the user to carry out specific tasks assigned to his/her/its role.*	*Registered staff members and their assigned roles with related permissions through Role Based Access Control to make use of the full interactive TUDesc application (Extended) or a sublicence such as ESViewerOnly.* *Contact person to carry out invoice, financial administration and handling of the TUDesc License of Use.*	*Storing of user name, email address, first name, last name, encrypted password, and institute.* *Storing of contact person's email address, first name, last name, phone number, institute's address, postal code.*	*Storing of license number, date from, date till, license type (e.g. ESViewerOnly, Extended), paid on date, amount, discount, quantity, invoice sent date, reminder sent date, payment confirmation sent date, email address of contact person.*

Appendix B: Permission for processing data by Google Cloud Data Processing Service

Sub-processor deployed by the Processor to process data	**Category of data to be processed by sub-processor**	**Type of processing**	**Country in which sub-processor is based**
Google Cloud Services: *Name of Google Kubernetes Engine: tudesc-cluster* *Location type: Zonal* *Control plane zone: Europe-west4-a*	*Personal data as is described in Appendix A* *Education spaces data, such as dimensions, lay-out, equipment, photos, generated pictures, configuration, properties, and dashboard parameters*	*Storing of personal data as described in Appendix A* *Storing of space data* *Calculation and generation of readability and ergonomic sightlines* *Generation of statistics based on available data to report on dashboards*	*Datacenter Google Eemshaven* *Address: Oostpolder 4, 9979 XT, Eemshaven, The Netherlands*

The Google Cloud Data Processing Addendum is incorporated into the Agreement **tudesc-cluster** (as defined on https://cloud.google.com/product-terms) between Google and TUDesc BV.

The Google Cloud Data Processing Services maintains a list of the sub-processing agreements for the **tudesc-cluster**.

During the Term of the agreement the Google Kubernetes Engine Service Level Agreement (SLA) provides a Monthly Uptime Percentage for the Zonal Cluster as is mentioned on https://cloud.google.com/kubernetes-engine/sla.

Appendix C: Security Measures

Security policy	• User email addresses, invoice email address, and passwords are stored in an encrypted way:
	  ○ TUDesc superusers are able to reveal user names and email addresses on request, but not able to reveal the passwords.
	• Confidential device features such as hostname, MAC address, and IP address are preferably not stored in the TUDesc database:
	  ○ These measures are for reducing and preventing unnecessary risks of vulnerable data being present on places where these do not have to be stored.
	  ○ The Controller may decide to store such confidential data for making use of specific TUDesc functionalities.
	  ○ Authorised users only with appropriate assigned roles and rights are allowed to work with the confidential data.
	  ○ The controller institute itself remains responsible to store and process such confidential device data in TUDesc.

Risk analysis	• The TU Delft checklist for Data Protection Impact Assessment (DPIA), based on both European Data Protection Authorities and Dutch Data Protection Authority, resulted in … *"The processing of personal data is not likely to lead to a high risk for the data subjects. It is not necessary to perform a DPIA."* • A daily back-up is done that shall be removed after seven days.
Change management	• Testing a provisional change, such as an upgrade or versioning, is conducted on a separate system and network. • When changes take place, such as upgrades or versioning, an extra back-up is made beforehand. • Bugs are solved as soon as possible without prior notice. • Minor changes, if applicable, take place every one to three months with announcements on the TUDesc website. • Major changes, if applicable, take place in non-working periods outside office hours with email communication to all users.
Continuity management	• Cloud containers of sub-processor take care for continuity and load-balancing of system and database. • Alive-ping every hour when API connections are in place for collecting AV system logs and a warning-email to the institute administrator in case the data train fails.
Confidentiality through assigned rights and roles	ESViewerOnly license has two Role Based Access Control actors: • Administrator: ○ Responsible for institute customization settings, such as logo, accessible colours, campuses, buildings, and spaces.

	○ Responsible for appearances of overview and detail pages with settings such as (bilingual) title headers, selection filters, sub-lists with features, order of columns and assets, datasets to be displayed, and alternative texts for the visually disabled. ○ Responsible for assigning delegate roles to users. ○ Responsible for assigning institute-wide manuals and documents. ○ NB: Administrator may fulfil the Delegate tasks as well. • Delegate: ○ Responsible for space data collection to show the current state of audiovisual installations and assets. ○ Responsible for space photographs and pictures. ○ Responsible for assigning specific space manuals and documents. TUDesc Extended or Full License has the following Role Based Access Control actors. More than one role may be assigned to one person: • Administrator: ○ Responsible for assigning groups, roles and rights to users, and able to change all space, asset, and device TABs in the admin pages. ○ Responsible for dashboards Overview Spaces, Assets Values & Costs, CO2 Equivalence, and Operational Use. ○ Responsible for assigning institute-wide manuals and documents. ○ Responsible for the Presence API i.e. API_PRESENCE_GROUP ○ Responsible for the Coordinatres API i.e. API_COORDINATES_GROUP ○ Responsible for the avlog API i.e. API_AVLOG_GROUP ○ NB: Superusers only are able to assign registered users a temporal superuser status for AV, Furniture, IT, Facilities, or Equipment to add models not yet available. • Asset Manager: ○ Responsible for furniture and able to change the Segments, Tables, Chairs, and Desks TAB admin pages. • Space Manager: ○ Responsible for building parameters and able to change Space Conditions, Doors, Windows, and Obstructions TAB admin pages. • IT Manager: ○ Responsible for information technology and network parameters, and able to change Hall Computers, Student PCs, Study Workplace Monitors TAB admin pages, as well as VLANs, video cards and software. ○ Allowed to import and export computers in single and batch formats. • Facility Manager:

	○ Responsible for available facilities and able to change Chalkboards, Whiteboards, and Traffic TAB admin pages. • AV Manager: ○ Responsible for audiovisual presenter and communication apparatus, and able to change Projectors, Displays, Interactive Boards, and Screens TAB admin pages. ○ Responsible for Image System Contrast Ratio Measurements. • AV-IT specialist: ○ Responsible for AV-IT Equipment and able to change AV Equipment TAB admin pages and devices such as Amplifiers, AV racks, Cameras, Controllers, Converters, En/Decoders, Extenders, Loudspeakers, Microphones, Operation and Signage Panels, Audio Processors, Recorders, Switchers, Video Processors, Visualizers, and other equipment. ○ Allowed to list and search through on premise stored but promptly loaded AV-IT devices. • General Task Assignments: ○ AllowConfiguratorView are default user rights to look-up spaces in TUDesc. ○ AllowConfiguratorSave allows to save changes made in available spaces. ○ AllowConfiguratorSaveAs allows saving a copy as new space. ○ AllowConfiguratorDimensions allows to change space depth, width and height of the spaces. ○ AllowConfiguratorCreateNew allows creating new spaces.

Access security

Physical access security	• The TUDesc database is made available via the Google cloud server in Eemshaven Data Centre in Groningen, The Netherlands. It is not possible to enter or visit the building due to the highly safeguarded environment.
Logical access security	• Access to the administrator pages is with username and password, and double authentication. • Connection with the TUDesc application is done via https, which end-to-end encrypts the online traffic over the network for secure communication. • Users are automatically logged out after 60 minutes of inactivity.
Life-cycle user accounts	• Registered users of an institute having a non-active licence are removed from the TUDesc database 15 months after the License of Use has stopped. • A grace period of 2 months is allowed in case payments are not done in time before a definitive access stop is conducted.

Confidentiality and data integrity

Privacy policy	• Personal data is handled confidentially and will not be shared to third parties. • No cookies are used for tracing, only for configuration purposes in order to maintain user settings.
Back-up/restore provisions	• Following the sub-processor specification for Zonal Clusters.

Incident response, reporting and remediation

Incident management	• Severe incidents will be reported within 24 hours in a format as given in Appendix D. • Remediation and mitigation will take place immediatly after discovery.

Software development life cycle

Development Strategy and Procedure	• The TUDesc application and its parts are developed in Django with Python, Javascript, HTML, and mySQL database. • Definition of wishes, demands, and new features are collected through email at Info@tudesc.com or personal contact. These are described and decomposed into issues and added to https://gitlab.com. Planning and Priority are placed into mile stones. • Design for webpages and coding development are done on a system completely isolated from production and test systems. • Testing quality, performance, and reliability is conducted on a test server in a separate network. • Deployment follows the order of change management, also manuals and additional documents are added when applicable. • Maintenance and versioning follow change management procedures.

TUDesc

Appendix D: Incident Management

The Processor reports severe incidents to the Controller within 24 hours after they are discovered. The following persons may be contacted in connection with reporting incidents:

Primary contact person	Secondary contact person
Marcel Heijink	Piet van der Zanden
Chief Technical Officer	Chief Executive Officer
m.j.heijink@tudelft.nl	a.h.w.vanderzanden@tudelft.nl

In reporting incidents to the Controller, the Processor will use the following format or at least provide information as is referred as in the table below. Reporting to contact person of Controller institute.			
Name	Your contact person		
Title			
E-mail address			
Information about the incident			
Summary of the incident	What has happened [*theft, loss of data, malware, hack, DDoS, accidental publication of data]*, in which way [*through internet, e-mail, external attack and so on*], and how the incident was discovered		
Nature of the incident	[*Inspection by unauthorised persons, data copied or downloaded, changes made, date deleted or destroyed, theft of data, not known yet*]		
Date and time of the incident	When or during which period the incident occurred		
Date and time of discovery	When the incident was discovered		
Data subjects	The persons whose data was involved in the incident		
Number of subjects	If appropriate, an estimate of the number of people		
Which types of personal data		Yes	No
	Personal data, e.g.: user name, email address, first name, last name, institute		
	Contact information, e.g.: email address, telephone number, postal address, city		
	Identification information, e.g.: user-ID, password		
	Licence data, e.g.: number, type, date, amount		
Which actions have been taken	Description of which actions have been taken to address the incident and to prevent further incidents		
Which measures have been taken	Description and explanation of which security measures apply to the personal data in question		
International aspects	Does the incident relate to persons in other EEA countries?		