MOHOLY-NAGY
művészeti egyetem
university of art and
design budapest

PRIVACY POLICY OF
MOHOLY-NAGY UNIVERSITY OF ART AND DESIGN BUDAPEST (MOME)

Approved by:	Zsuzsanna Kun, CEO
Entered into force:	4 October 2022
Responsible department:	Office of the Chief Executive Officer
Mandatory review:	4 October 2024

PRIVACY POLICY OF MOHOLY-NAGY UNIVERSITY OF ART AND DESIGN BUDAPEST

The CEO of the Moholy-Nagy University of Art and Design Budapest (hereinafter the University or MOME), pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), Act CXII of 2011 on Informational Self-determination and Freedom of Information (hereinafter the Information Act) and Act CXIX of 1995 on the Processing of name and address data for research and direct marketing purposes, hereby establishes the following Privacy Policy.

Chapter I
General provisions

The purpose and scope of the Policy
Article 1

(1) The purpose of this Policy is to define the lawful mode of operation of the registers and records kept by the University in the context of handling and processing personal data, to ensure compliance with the constitutional principles of data protection, the right to information self-determination and the requirements of data security, to prevent unauthorised access, alteration and unauthorised disclosure of data, and to specify the information and data that the University may process concerning natural persons and the purposes for which it may use them. This Policy also aims to specify the internal functioning of the University in relation to the processing of personal data in the context of its activities.

(2) The applicable regulatory environment – in particular the following legislation – shall be used in the course of interpreting, applying and implementing of the provisions of the Policy:
   a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter the General Data Protection Regulation or GDPR);
   b) Act CXII of 2011 on Informational Self-determination and Freedom of Information (hereinafter the Information Act);
   c) Act CXIX of 1995 on the Processing of name and address data for research and direct marketing purposes.

(3) The content of the legislation currently in effect shall be applied to all actions and activities relating to personal data.

(4) The controller:
   Name of the controller: Moholy-Nagy University of Art and Design Budapest
   Controller's registered office: 1121 Budapest, Zugligeti út 9-25.

(5) If it is not possible to decide whether or not a specific piece of data qualifies as personal data or sensitive personal data, such data shall be considered as having such character until the respective internal decision is taken. The classification of the data as personal data or sensitive personal data shall be decided by the CEO.

(6) The processing of personal data must be carried out in full compliance with the law and with this Policy and in such a way that the activity

a) entails the processing of personal data only to such an extent and for such time as is absolutely necessary for the purposes for which such personal data are collected;
b) does not jeopardise the security of personal data and the rights and freedoms of the natural person data subjects;
c) when considering the risks of the activity, data protection is to be a high priority, and the assessment of the related impacts must always take the maximum potential impact into account and avoid underestimating the risks.

(7) This Policy applies to:
a) the University and all departments and organisational units of the University where personal data are processed;
b) all employees of the University and all persons involved in its activities, including in particular its agents and contractors and contractual partners, who process personal data or who become aware of personal data in the course of their activities carried out at the University; and
c) departments and organisational units processing data of public interest and data accessible on public interest grounds.

(8) The University shall process personal data in accordance with the provisions of this Policy. The University shall ensure that its employees are familiar with this Policy.

(9) This Policy applies to both electronic (automated, i.e. implemented by electronic means within the meaning of the General Data Protection Regulation) and manual (hard copy/paper-based) processing of personal data. This Policy shall not apply to processing operations that do not relate to personal data.

(10) This Policy – in terms of its provisions relating to the protection of personal data – shall not apply to institutions maintained by the University, business associations owned by the University, or any organisation with independent legal personality that operates with the University's participation or is related to the operation of the University (hereinafter "organisation"), but the University, as the maintainer, owner, participating member or cooperating partner of such organisations, assists, encourages and expects these organisations to develop their own data protection systems in accordance with the data protection principles set out in this Policy.

(11) For all relevant contracts, the CEO shall be obliged to ensure that the party entering into a contract with the University is made aware of the provisions of this Policy and the currently effective data processing notice.

Definitions
Article 2

(1) For the purposes of this Policy, the definitions used shall, subject to the exceptions set out in paragraph (2), be those set out in Article 4 of the General Data Protection Regulation.

(2) In addition to paragraph (1), for the purposes of this Policy:
a. Employee: a person who is employed by the University or has another employment relationship with the University;
b. data of public interest: information or knowledge not covered by the definition of personal data, recorded in any way or form, which is held by a body or person performing a state or local government function or other public function specified by legislation, and which relates to the activities of that body or person or arises in connection with the performance of its public function, irrespective of the way in which it is processed or handled, whether it is individual or

collective, including in particular information on its powers, competences, organisational structure, professional activities, including an assessment of their effectiveness, the types of data held and the legislation governing its operation, as well as on its financial management and the contracts concluded;

c. data accessible on public interest grounds: any data not covered by the definition of data of public interest, the disclosure, accessibility or making available of which is required by law on the grounds of public interest.

The manager responsible for data processing

Article 3

(1) The heads of the University's organisational units (hereinafter collectively "manager responsible for data processing") shall be responsible for the fulfilment of the obligations of the University as data controller or data processor and for the preparation for the necessary decisions of the CEO, through the implementation of the activities falling within the competence of the organisational units under their direct responsibility.

(2) The manager responsible for data processing shall be responsible in particular for the following:

a. decision on the necessity, purpose and duration of the processing;
b. preparation of a data protection risk analysis and/or impact assessment;
c. regular review of the processing;
d. documentation of the circumstances justifying the lawfulness of the processing (in particular, consent and balancing interests);
e. if it becomes necessary to involve a third party in the processing, to notify the managing director and to prepare the necessary data processing contract or joint controller agreement;
f. preparing information for and informing data subjects;
g. in the event of a personal data breach, assessment of the breach and determination of the action to be taken in response.

(3) If it cannot be clearly established which manager responsible for data processing is responsible for a particular data processing-related task, or if the competence of more than one manager responsible for data processing is affected, the CEO shall designate which manager responsible for data processing shall be responsible for that task and may determine how the tasks to be performed shall be shared. In the absence of designating or sharing tasks, the managers responsible for data processing shall be jointly responsible for the tasks relating to the data processing actions carried out by their organisational units.

The data protection officer

Article 4

(1) The University employs an independent data protection officer, appointed in accordance with Articles 37-39 of the General Data Protection Regulation, who cannot be instructed in the performance of their data protection duties and who, in this capacity, is directly supervised by the managing director and reports to the Chief Executive Officer.

(2) The data protection officer assists the Chief Executive Officer, the manager responsible for data

processing and the employees of the University on data protection issues, in particular:

a. providing information and technical advice to staff carrying out processing operations in relation to obligations as per the General Data Protection Regulation and other EU or national data protection provisions;
b. monitoring and checking compliance with the General Data Protection Regulation, other EU or Member State data protection provisions and the University's internal rules on the protection of personal data, including the assignment of responsibilities;
c. participating in and coordinating awareness-raising and training for employees involved in data processing operations;
d. facilitating the exercise of the rights of the data subject, participating in the investigation of any data subject's complaints and initiating the necessary action to redress the complaint with the University;
e. cooperating with the Authority and acting as a contact point for it;
f. liaising with external authorities and organisations on data protection related issues, providing them with the necessary information and cooperating with the authorities conducting the investigation in the event of external investigations;
g. reporting annually to the CEO on their activities, the University's processes involving personal data and the status of compliance with data protection obligations;
h. maintaining the Company's data protection and personal data breach registers.

(3) The data protection officer shall be ensured access to all information and data necessary for the performance of their data protection duties.

Chapter II
Data Protection Provisions

Data Protection Principles
Article 5

(1) Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data shall be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to

implementing the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f) processed in a manner that ensures appropriate security for the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures ('integrity and confidentiality').

(2) The controller shall be responsible for, and be able to demonstrate compliance with the principles of data processing ('accountability').

(3) Other principles not specified in the GDPR, according to which and in the light of which the controller carries out processing activities:

a) Principle of data security: The controller is obliged to design and implement the data processing operations in such a way as to ensure the protection of the privacy of data subjects in the application of the law applicable to data processing. The University is obliged to ensure the security of personal data processed by it in its capacity as data controller or data processor; furthermore, it shall take the technical and organisational measures and establish the procedural rules necessary to enforce data protection legislation and the provisions of this Policy.

b) Principle of transparency: the information provided to the public or to the data subject must be concise, easy to understand and accessible, and must be drafted in clear and plain language and, where appropriate, in addition to that, the information must also be presented in a visualised form. This provision also applies to information relating to the processing of personal data. This principle applies in particular to

ba) information to the data subject on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing of the data subject's personal data, as well as

bb) information that the data subjects have the right to obtain confirmation and communication on personal data concerning them that are being processed. Natural persons must be made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

c) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller shall provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject must be informed of the existence of profiling and its consequences. Where the personal data are collected from the data subject, the data subject must also be informed whether or not they are obliged to provide the personal data and of the consequences if they fail to provide such data.

d) Principle of documentation: All activities and operations carried out in relation to data media containing personal data processed by the University must be documented in order to ensure that the trail of personal data and the location of personal data can be traced accurately.

e) Principle of responsibility: Employees who are involved in the processing of personal data are obliged to be familiar and fully comply with the provisions of the law on the protection of

personal data and of this Policy. Those violating the data protection rules shall be subject to disciplinary, labour law, misdemeanour, civil and criminal liability, in accordance with the provisions of the applicable legislation.

Rights of data subjects and their enforcement

Article 6

(1) Under the legislation on data protection, the data subject has the right to:

a) request access to their personal data;
b) request rectification of their personal data;
c) request erasure of their personal data;
d) request the restriction of the processing of personal data;
e) object to the processing of their personal data;
f) request data portability;
g) object to the processing of their personal data (including objecting to profiling; and other rights relating to automated decision-making); and to
h) withdraw their consent or lodge a complaint with the competent supervisory authority.

(2) Right of access:

a) The data subject has the right to obtain confirmation from the University as to whether or not personal data concerning them are being processed. If such processing is ongoing, they may also request access to their personal data.
b) The data subject has the right to obtain a copy of the personal data which are the subject of the processing. For identification purposes, the University may request additional information from the data subject or charge a reasonable administrative fee for additional copies.

(3) Right to rectification:

The data subject shall have the right to obtain from the University the rectification of inaccurate personal data concerning them. Depending on the purpose of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

(4) Right to erasure ('right to be forgotten'):

The data subject has the right to request the University to delete their personal data and the University shall be obliged to delete such personal data if one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed by the University;
b) the data subject withdraws their consent on which the processing is based according to point (a) of Article 6(1) of the GDPR, or point (a) of Article 9(2) of the GDPR, and where there is no other legal ground for the processing;
c) the data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR;
d) the personal data have been unlawfully processed by the University;
e) the personal data must be erased for compliance with a legal obligation in European Union or Hungarian law to which the University, acting as the controller, is subject;
f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

(5) Right to restriction of processing:

The data subject has the right to request the restriction of the processing of their personal data. In this case, the University will identify the personal data subjected by the restriction which, with the exception of storage, shall only be processed:

a) with the data subject's consent or
b) for the establishment, exercise or defence of legal claims or
c) for the protection of the rights of another natural or legal person or
d) for reasons of important public interest of the Union or of a Member State.

(6) Right to object:

a) The data subject has the right to object, on grounds relating to their particular situation, at any time to the processing of personal data concerning them by the University that is based on point (e) or (f) of Article 6(1) of the GDPR, including profiling based on those provisions, or to request the University not to process their personal data any longer.
b) In addition, where the University processes the personal data of the data subject on the basis of a legitimate interest within the meaning of Article 6(1)(f) of the GDPR, the data subject has the right to object at any time to the processing of their personal data for this purpose.

(7) Right to data portability:

The data subject has the right to receive the personal data concerning him or her provided, in a structured, commonly used, machine-readable (digital) format and the right to request the transfer of such data to another controller, where such transfer is technically feasible, without hindrance from the University.

(8) Right to withdraw the consent:

a) The data subject has the right to withdraw their consent at any time. Withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The data subject must be informed of this right before consent is given. It must be possible to withdraw consent in the same simple way as it is given.
b) If the data subject withdraws their consent given to the University for processing their personal data, the University may not be able to provide the requested services at all or only partially.

Conditions for the processing of personal data

Article 7

(1) Personal data may only be processed if all of the following conditions are met:

a) the legal basis for the processing fulfils one of the conditions of Article 6(1) of the GDPR, such as:
   aa) the data subject has given consent to the processing of their personal data for one or more specific purposes;
   ab) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   ac) processing is necessary for compliance with a legal obligation to which the controller is subject;
   ad) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

ae) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

af) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require the protection of personal data, in particular where the data subject is a child.

b) the need for the processing has been approved by the manager responsible for data processing;

c) a data protection risk assessment and, where necessary, an impact assessment have been carried out in relation to the processing – or, where the data protection impact assessment indicates that the processing is likely to present a high risk, even in the absence of measures to mitigate the risk, the supervisory authority (Hungarian National Authority for Data Protection and Freedom of Information, hereinafter the Authority or the NAIH) has been consulted and the processing has not been prohibited by the Authority;

d) the processing has been recorded in the internal data protection register or, after the processing has been started, it will be recorded without delay.

(2) In the case of processing sensitive data, in addition to meeting the conditions set out in paragraph (1), it is necessary that the data processing also complies with one of the requirements of Article 9(2) of the General Data Protection Regulation.

(3) If the processing of personal data becomes necessary for purposes other than the original purpose for which the data were collected, and if those purposes are compatible, no new legal basis for the processing operation need to be specified.

The following must be taken into account when deciding whether the purposes are compatible:

- the circumstances in which the personal data are collected,
- the relationship between the data subject and the Company (e.g. whether there is an inequality),
- the nature of the personal data (whether sensitive data or not),
- the consequences of further processing for the data subject, and
- whether appropriate safeguards are in place (e.g. encryption, pseudonymisation).

No specific assessment of the compatibility of the purposes is required where the further processing has been consented to by the data subject or is required by EU or national law. Further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes may be considered lawful.

Before starting the further processing for a different purpose, a reminder of the decision on the compatibility of the purposes and the criteria taken into account must be prepared and the data subject must be informed of the different purpose.

(4) For any processing where the purposes and means of processing are not determined solely by the University, the processing shall be further subject to the conclusion of a joint controller agreement between the two controllers pursuant to Article 26 of the GDPR, to which the CEO is authorised to act on behalf of the University.

(5) If the University acts as a data processor or intends to use a data processor (sub-processor) for the processing of data, and the tasks of the data processor are not – or not fully – provided for by law, a contract for the performance of the tasks of the data processor shall be concluded with the content determined in Article 28(3) of the General Data Protection Regulation.

(6) The employee responsible for data processing shall be responsible for:

a) preparation of the risk analysis required for the data protection impact assessment and the preparation of the impact assessment itself, based on the relevant methodology,

b) making recommendations in the course of the risk analysis and the impact assessment

ba) regarding the limits (e.g. personnel, time) on access to data;

bb) regarding the rules on data transfers (to whom, for what purpose, under what conditions);

bc) regarding other technical and organisational measures to be implemented in connection with the processing (e.g. the storage location of files or documents containing the data, password management rules for the use of the data storage devices, or limiting the use to the University's registered address).

The CEO shall decide on the recommendations made on the above points by approving the risk analysis and impact assessment forms.

(7) Only a reason or circumstance that meets the requirements specified by law, is directly related to, necessary for, or otherwise appropriate for the activities of the University may be specified as the purpose of data processing.

(8) The scope of the data processed shall be defined as the minimum necessary, but at the same time justified for the safe and responsible performance of the University's activities.

(9) The risk analysis required for the data protection impact assessment and, where justified (i.e. where the risk analysis indicates that the processing is likely to result in a high risk to the rights and freedoms of data subjects), the data protection impact assessment must be carried out by the employee responsible for the processing by the deadline set by the CEO.

(10) If the data protection impact assessment indicates that the processing is likely to result in a continuing high risk to data subjects in the absence of measures to mitigate the risk, the CEO must consult the Authority before starting the processing of the personal data. The employee responsible for data processing must be involved in the consultation; they shall review the risk analysis and the data protection impact assessment on the basis of the results of the consultation and the measures taken on the basis of the findings of the consultation.

(11) The risk analysis and/or impact assessment forms must be saved electronically by the employee who prepared them, after approval by the data protection officer, and sent to the CEO in digital format at the same time. Access to the information in the risk analysis and the impact assessment shall be limited to the employee who prepared them (or the person who took over their post of employment), the CEO and the data protection officer.

(12) The data of the internal data protection register shall be entered into the database by the data protection officer on the basis of the risk analysis and the impact assessment documents. The data protection register shall be checked by the CEO as necessary, but at least once a year.

(13) Where a type of processing, in particular using new technologies, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single impact assessment may address a set of similar processing operations that present similar high risks.

Data Protection Register

Article 8

(1) The commencement, modification and termination of the data processing operations and the technical tasks related to data processing must be notified to the data protection officer, who shall ensure that it is registered and the changes are entered in the data protection register. The register must be made available to the Authority on request.

(2) A review of the data processing operations contained in the data protection register should be carried out in justified cases, but at least by the last working day of February each year. This must include verification of the purposes of the processing, the interest balancing tests previously carried out, the findings of the risk analysis and of the data protection impact assessment. The review of the data protection register shall be coordinated by the data protection officer. Once the review has been completed, the up-to-date data of the register must be presented to the CEO, who shall approve the register, if they concur.

Data processing notices and their recording

Article 9

(1) Where personal data relating to the data subject are collected from the data subject, the controller shall inform the data subject by means of a data processing notice at the time of obtaining the personal data or, if not collected from the data subject, within a reasonable period of time from the date of obtaining the data, but no later than one month.

(2) The data processing notice must contain the information specified in Articles 13 and 14 of the General Data Protection Regulation.

(3) The data processing notices shall be prepared by the organisational units, where necessary, after requesting the opinion of the data protection officer.

(4) The organisational units shall ensure that the data processing notice is reviewed, and if necessary amended, by 31 December each year, and shall inform the CEO and the data protection officer thereof, electronically.

Register of data subject requests

Article 10

(1) The organisational units of the University shall keep a register of the exercise of the rights of the data subject under Articles 15-22 of the GDPR.

(2) The register shall contain:

a) the date of the data subject's request;
b) the date of the response to the request;
c) the date of performance/rejection;
d) the reason for the rejection.

Practical rules on the processing of personal data

Article 11

(1) Personal data may only be processed in full compliance with the internal rules set by the CEO and the legal requirements. In addition, any activity or phenomenon indicating that a person having a contractual relationship with the University or the data subject is not complying with the legal requirements relating to data processing shall be reported to the CEO without delay. In such a case, the performance of the contract shall be suspended until the lawfulness of the processing is

restored, in such a way that the data subjects affected by the particular data processing are not adversely affected, or the level of services provided by the University is reduced to the least extent possible.

(2) All employees must ensure that an appropriate legal basis is provided for the processing – in other words:
   a) the personal data are provided by the data subject and the data subject consents to their processing;
   b) the data are provided by a contractual partner of the University, in which case the lawfulness of the processing is ensured by the contract between the University and the partner (in which the University and the partner are identified as joint controllers);
   c) the University has the right to process the data by law;
   d) processing is carried out in the context of the conclusion of a contract to which the natural person data subject is a party;
   e) the University has a legitimate interest in the processing of the data, and the processing does not conflict with the interests or fundamental rights and freedoms of the data subject.

(3) All employees of the University are required to comply with the following practical rules regarding the processing of personal data:
   a) only the personal data strictly necessary for the performance of the work may be processed and transmitted, and it is the responsibility of the head of the organisational unit or directorate responsible for the given task to design the work processes accordingly (avoiding unnecessary data accumulation);
   b) when authorising IT access rights, it must be ensured that access to personal data is only granted to persons whose work absolutely requires access to the data or data set;
   c) paper documents containing personal data may only be transmitted in a sealed envelope;
   d) a document containing personal data sent by e-mail must be transmitted in such a way as to ensure that it can only be viewed by the authorised person, by including a warning sentence in the body text of the letter, as follows: "The attachment contains personal data, which may be accessed only and exclusively by the addressee of the letter.";
   e) a document containing personal data may only be stored on shared drives used by the organisational units if it is ensured that only authorised persons have access to it and, in the case of shared drives, the head of the respective organisational unit shall be responsible for the obligation as per this Section.

(4) If a breach of the data processing rules is detected, every employee is obliged to report it to the CEO without delay. On the basis of the notification, the CEO shall investigate the data processing practices in question or have them investigated and, on the basis of the results, take the necessary measures to ensure secure data processing that safeguards the rights and freedoms of data subjects.

(5) In line with Article 32 of the GDPR, the University – taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons – shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:
   a) the pseudonymisation and encryption of personal data;
   b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

Article 12

(1) Personal data must be deleted if

a) the period set for processing has expired;

b) the purpose of the processing has been fulfilled or the given purpose could be achieved without processing the personal data;

c) the data subject so requests;

d) with regard to the technical tasks of data processing, the controller shall instruct the University in writing;

e) the University is required to do so by law or by a court or administrative decision.

(2) Notwithstanding paragraph (1), data that may be necessary for the performance of the University's contractual or statutory obligations shall not be deleted.

(3) In all cases, the deletion of data shall be approved by the CEO or the data protection officer – except for automated deletions of data that involve electronic databases or documents and for which the deletion routines have been approved in advance by the CEO.

(4) The deletion of personal data must be carried out in such a way as to exclude the possibility of the deleted data being subsequently restored and accessed. Accordingly:

a) paper-based documents containing personal data

aa) shall be destroyed in their entirety (e.g. by shredder);

ab) if the complete destruction of the document is not justified, erasure shall be ensured by rendering the personal data unreadable, in such a way that the electronic copy of the paper - based document is also deleted or replaced by the version containing the unreadable data;

b) electronic documents containing personal data

ba) shall be deleted in their entirety, or

bb) if their complete deletion is not justified, the data to be deleted shall be removed from it in such a way that the version of the electronic document containing personal data cannot be recovered.

Electronic documents and databases also need to be deleted from backups, or a recovery protocol should be provided that does not restore the files in question and does not allow access to the contents of the backups (not even to third parties such as those performing system administrator tasks).

(6) The employee who directly processes the data shall be responsible for deleting the data.

Article 13

(1) Anyone who, in the course of their work, has a question about the processing of personal data, such as if they are uncertain about the processing or the classification of data as personal data, or become aware of a breach of the rules on data processing, must, without delay, contact the manager responsible for data processing or the data protection officer to clarify the matter, who

will take the necessary measures to ensure that the conditions for secure processing are established in order to safeguard the rights and freedoms of data subjects.

(2) Statements and instructions regarding data processing must be made in writing. Where, in view of all the circumstances of the case, urgent oral communication is justified, the communication must be made (repeated) in writing without delay after the circumstances giving rise to the oral communication have ceased to exist. Communication by e-mail, SMS and other messaging applications and services within the University is considered as written if it is available in an unaltered and retraceable form for the required period of time.

(3) In actions related to data protection, the utmost effort must be made at all times to ensure that compliance with this policy and with the legal requirements can be demonstrated, in particular with respect to the following:

a) the data subject's consent to the processing,
b) the performance of the interest balancing test for processing based on legitimate interest,
c) the data subject's complaints and requests, in particular the management of the data subject's requests regarding access to the details of the processing, the erasure, rectification or transfer of data or the restriction of processing or the objection to processing,
d) the notification of data breaches to data subjects,
e) the data protection and personal data breach register,
f) the controller's instructions for the processing activities.

(4) No performance from any third party may be accepted if such performance contains personal data which the University cannot guarantee to process lawfully. This provision must be included in the contractual agreement concluded with third parties.

Data breach-related procedure
Article 14

(1) Anyone who becomes aware that a data breach has occurred must report it to the CEO and to the relevant manager responsible for data processing or the data protection officer without delay, but no later than 12 hours after becoming aware of the breach.

(2) The manager responsible for data processing shall, with the involvement of the data protection officer, ensure the investigation of the personal data breach concerning data processed by the organisational unit under their control, the assessment of the risks associated with the personal data breach and, where necessary, the preparation of the documentation related to the notification of the personal data breach to the Authority and the information to be provided to the data subjects. The investigation of the personal data breach must identify the technical and organisational measures to avoid further personal data breaches. The data protection officer must become involved in the procedure conducted to investigate the personal data breach.

(3) The findings of the investigation of the personal data breach shall be reported to the CEO, who will decide on further action to be taken in relation to the personal data breach.

(4) If, on the basis of the risk assessment, the personal data breach is likely to pose a risk to the rights and freedoms of the data subject(s), it shall be notified to the Authority without delay and at the latest within 72 hours of the occurrence or becoming aware of the personal data breach, with the content as referred to in Article 33 of the General Data Protection Regulation. Where such notification cannot be achieved within 72 hours, the reasons for the delay must accompany the

notification. Where this risk is likely to be high, the data subject(s), in addition to the Authority, must also be notified in accordance with Article 34 of the General Data Protection Regulation.

(5) The data protection officer shall enter the personal data breach in the data breach register. The data breach must be recorded in the register even if there is no reason to notify it to the Authority or to inform the data subjects of it.

(6) Documents related to the assessment of the personal data breach must be saved in electronic format, accessible to the CEO and the data protection officer.

(7) If the personal data breach occurred in the course of the University's data processing activities, it must be reported to the data controller without undue delay after becoming aware of it.

Processing of sensitive data
Article 15

(1) Sensitive data may only be processed in the cases provided for in Article 9(2) of the GDPR (in particular on the basis of the data subject's explicit consent) and only if the conditions set out in Article 7(1) of this Policy are met.

(2) Access to sensitive data may only be granted to the CEO, the employee directly performing the processing action and/or the employee who replaces them. Access to other employees or to external third parties under contract with the University may only be granted in particularly justified cases.

(3) In the case of sensitive data, risks related to data processing cannot be excluded in the framework of a data protection impact assessment or in the framework of personal data breaches, nor can the related activities be assessed as likely to be risk-free.

(4) In the case of sensitive data, the imposition of technical and organisational measures justified by the nature and form of the data and the risks involved in their processing cannot be avoided.

Technical rules for data processing and rules on data processing security
Article 16

(1) The security measures necessary to prevent the loss of and destruction, damage and unauthorised access to data shall be specified before the commencement of the data processing (or the data processor's activities), in the course of the risk analysis, in a manner appropriate to the characteristics of the processing and the nature of the personal data, and shall be reviewed regularly, even in the absence of any personal data breach involving the data concerned.

(2) Paper-based documents containing personal data shall only be kept according to the storage scheme and in the storage devices set out in the records management policy and may only be removed from the University's premises with the permission of the Chief Executive Officer.

(3) Personal data stored in electronic form or documents containing personal data may only be handled and processed on password-protected computers, in accordance with the provisions of the University's currently effective information security policy. The transmission of such documents or databases to an external storage facility or mailing system, or their use, opening or storage on other devices potentially accessible by third parties is prohibited.

(4) Such security solutions must be installed on the computers referred to in paragraph (2), which ensure the IT security needs in relation to the subject matter of the processing and the nature of the processing. The specific needs are to be determined on the basis of the results of the data

protection impact assessment.

(5) Efforts must be made to ensure that electronic documents or databases containing sensitive personal data are stored or processed only on the University's own devices. The provisions of paragraph (2) shall apply mutatis mutandis to these devices.

(6) Backups of documents or databases containing personal data (or backups also containing – among others – such documents or databases), even with appropriate encryption, shall only be stored in an environment that supports the enforcement of high level data security guarantees and does not pose a risk to the security of the data.

Chapter III

Complying with requests for access to data of public interest and to data accessible on public interest grounds; disclosure of data of public interest and data accessible on public interest grounds

Rules on the public disclosure of data subject to mandatory disclosure

Article 17

(1) The University shall make the mandatory data specified in Annex 1 of the Information Act available on the University's website in digital form, accessible to anyone without identification, without restriction, in a printable form, in a way that it can be copied in detail without data loss or distortion, free of charge, for viewing, downloading, printing, copying and network transmission. Disclosed data must be protected against unauthorised alteration, deletion, destruction or damage. Access to the published data may not be made subject to the provision of personal data.

(2) The data related to the University's activities, as defined in Annex 1 of the Information Act, shall be published in accordance with the Chancellor's Instruction No. 3/2018 (I.31.) on the Rules of Procedure for the Disclosure of Data of Public Interest. Updating the data shall be initiated by the responsible person determined in the instruction, at the intervals specified in the instruction.

(3) Other data to be disclosed may be specified by law (hereinafter the "special disclosure list").

(4) The Chief Executive Officer – after obtaining the opinion of the Authority – and legislation may determine additional categories of data to be disclosed with effect for the University, or for bodies or parts of bodies under its control or supervision (hereinafter the "specific disclosure list").

(5) The Chief Executive Officer shall review the specific disclosure list annually on the basis of the data of data requests submitted for data of public interest not included in the disclosure list and shall add further data to the list based on the data requests received at a significant rate or quantity.

(6) The Authority may also propose the establishment of special or specific disclosure lists.

Access to data of public interest and data accessible on public interest grounds processed by the Foundation

Article 18

(1) The University shall make the data of public interest and the data accessible on public interest grounds processed by the University and not included in the disclosure lists available to any person upon request, subject to the exceptions set out in the Information Act.
Such a request can be made at the following contact points of the University:

By post: Moholy-Nagy University of Art and Design, 1121 Budapest, Zugligeti út 9-25.

Electronically: jog@mome.hu

In person (orally): During working hours at the University's registered address

(2) Requests made orally in person must be recorded in writing in accordance with Annex 1 (Request Form) of this Policy, no later than 2 working days after the respective request was made.
Unless otherwise provided by law, the personal data of the person requesting the data may only be processed to the extent necessary to fulfil the request and to pay the costs due for the copying. After the expiry of the time limit set out in the Information Act or after the payment of the costs, the personal data of the person requesting the data must be deleted without delay.

(3) Data of public interest or data accessible on public interest grounds shall not be disclosed if it qualifies as classified information under Act CLV of 2009 on the Protection of Classified Information.

(4) Requests submitted in writing, by post or electronically must include the following information:
   a) the name of the person requesting the data (in the case of a non-natural person, the name of the entity that requested the data),
   b) the contact details of the person requesting the data at which any information relating to the data request may be provided to them,
   c) the means by which the data request is to be fulfilled (e.g. paper-based copy, electronic copy, visual inspection, etc.).

(5) Data created or recorded in the course of the procedure conducted for making a decision falling within the University's powers and responsibilities and used to support and justify the decision shall not be made public for 10 years from the date on which it was created. Access to such data may be authorised by the head of the organisational unit or body which holds the data, by weighing the public interest served by disclosure or non-disclosure.

(6) If the data request is unclear, the person making the request must be asked to clarify the request. If the person making the request does not respond to the call for clarification, the request must be deemed withdrawn. The person making the request must be warned of this in the call.

(7) The University shall comply with a request for access to data of public interest within the shortest possible time from the date of becoming aware of the request, but not later than within 15 days. If a significant amount or quantity of data is requested, the deadline may be extended on one occasion, by 15 days. This must be notified to the data protection officer within 15 days of receipt of the request.

(8) The request received must be forwarded by the controller to the Legal Department within 2 days. If the request has been submitted to an organisational unit other than the one responsible for providing the data, the Legal Department will designate the organisational unit responsible for providing the data and for compiling the response, without delay, depending on the subject of the request received (within a maximum of 3 days), and will forward the request for data of public interest to the head of the organisational unit together with the designation.
If the request can be fulfilled, the organisational unit designated to provide the data shall prepare the data and, if requested by the requestor, the copies of the data for inspection or transfer, and shall send its proposal, including the amount of the expenses to be reimbursed (if any), to the CEO for decision-making through the Legal Department. The Legal Department shall keep a public

interest data provision register on the basis of the information provided by the organisational unit that fulfils the request.

(9) The person requesting the data may receive a copy of the documents or part of the documents containing the data. The University may require expenses to be reimbursed for the fulfilment of the data request up to the amount of the costs incurred in connection with the request, the amount of which shall be notified to the requestor by the Legal Department prior to the fulfilling the request. The requestor shall declare within 30 days of receiving the information whether or not they maintain the request. The period from the time the information is provided until the time the University receives the requestor's declaration shall not count towards the time limit for fulfilling the data request. If the requestor maintains their request, they must reimburse the expenses to the University with a payment deadline of at least 15 days.

(10) The amount of the expenses to be reimbursed shall be determined on the basis of the Government Decree on the amount of the expense reimbursement for the fulfilment of a request for data of public interest [at the time of adoption of this Policy: Government Decree no. 301/2016 (IX. 30.)].

(11) If the document containing the data of public interest also contains data that are not allowed to be disclosed to the requestor, such data must be made unrecognisable on the copy.

(12) The data request must be fulfilled in an intelligible form and, where the data controller is able to do so without disproportionate difficulty using the technical means or method preferred by the requestor. If the requested data has been previously disclosed in electronic form, the request may be fulfilled by indicating the public source of the data.

(13) The Legal Department shall notify the requestor of the rejection to fulfil the request, together with the reasons for the rejection and the information on the legal remedies available to the requestor under the Information Act, in writing within 15 days of receipt of the request – or by e-mail if the requestor has provided their e-mail address in the request – after consultation with the organisational unit designated to provide the data. The Legal Department shall keep a register of rejected requests and the reasons for rejection and shall inform the Authority of the information contained in that register by 31 January each year.

(14) The University shall not be obliged to comply with the request to the extent that it is identical to a request for the same set of data submitted by the same requestor within one year, provided that there has been no change in the data in the same set of data; or, if the requestor does not provide their name, or its name in the case of a non-natural person and their/its contact details where any information and notification relating to the request may be provided.

Chapter VI
The electronic surveillance system operated on the University premises

Operation of the electronic surveillance system

Article 19

(1) The electronic surveillance system is operated by the University itself. The Rector, the CEO and the persons authorised by them in writing, and the competent employees of the security service provider under contract with the University shall be entitled to access the recorded data.

(2) The electronic surveillance system serving the protection of persons and property may only be used in the areas of the University buildings open to the public.

(3) Natural persons who enter the areas of the University open to the public are deemed to have

provided their informed consent to the use of the electronic surveillance system, implied by their conduct.

Scope and use of data collected during the monitoring

Article 20

(1) Movement within the University and its buildings is monitored by an electronic surveillance system, which produces images containing personal data.
(2) The processing is adequate, relevant and limited to what is necessary for the data processing purposes indicated – i.e. the safety of people and the protection of life and property.
(3) The use of the images recorded during the operation of the electronic surveillance system is subject to data protection rights and to the restrictions set out in the law on the protection of property. In relation to the recordings, use of the recorded images as evidence in judicial or other official proceedings shall be considered as use.

Data security measures

Article 21

(1) The screen used for viewing and reviewing the images will be positioned so that it cannot be viewed by any person other than the authorised person while the images are being displayed.
(2) The surveillance and the review of the recorded images may only be carried out for the purpose of detecting infringing actions and initiating the necessary measures to stop them. The images broadcast by the cameras shall not be recorded by any device other than the central recording units.
(3) Access to the stored images may only be made in a secure manner and in such a way that the identity of the person who has carried out the processing can be identified. A record must be taken of the subsequent inspection, review or transmission of the camera recordings, which shall contain the data used to identify the camera recording or access data (device ID, time, duration), the reason and legal basis for the inspection or transmission and, in the case of transmission, the recipient of the data. If the reason underlying the entitlement (access rights) has ceased to exist, access to the stored recordings/images must be terminated immediately.
(4) Camera recordings must be stored on a secure, separate server. After the retention period (30 days), the data shall be deleted automatically. No backup is made of the recordings.
(5) After an unlawful act has been detected, measures must be taken to ensure that the recording of the act is stored and that the necessary official procedure is initiated without delay, and at the same time the authority must be informed that a recording has been made of the act.

Placement of cameras

Article 22

(1) The exact location of the cameras and the area they cover are set out in Annex 2 to the Policy.
(2) The operation of the cameras are indicated by information signs clearly visible to the data subjects. No hidden cameras are operated on the University's premises, and no cameras are located in areas where this may offend human dignity, in particular in toilets, washrooms and changing rooms. The

field of view of the cameras does not cover the work stations of employees or public space. The screen used to view the images is placed in a way that prevents unauthorised persons from viewing the camera image and, to this end, the screen is placed in a room under constant surveillance.

(3) Third parties wishing to enter the premises are informed of the use of the electronic surveillance system by means of pictograms placed in clearly visible places.

Data transfer and processing

Article 23

(1) The University shall, upon request, forward the images recorded by the cameras to the authorities or courts for the purpose of conducting the regulatory offence or criminal procedure.

(2) The legal basis for the transfer of data: Sections 261-265, 309 (1), and 315-317 of Act XC of 2017 on Criminal Procedure, and Sections 75 (1) (a) and 78 (3) of Act II of 2012 on Regulatory Offences, the Regulatory Offence Procedure and the Regulatory Offence Registry System.

(3) Economic entities that have a contract-based relationship with the University for the protection of persons and property shall qualify as data processors.

Rights of the data subjects

Article 24

(1) A person whose right or legitimate interest is affected by the recording of the images or the recording of their other personal data may request – within the retention period applicable in terms of the recording (*within 25 days, i.e. 30 days minus 5 days)* – that the data be not destroyed or erased, by justifying their right or legitimate interest. The recordings or other personal data must be sent without delay to the court or other authority upon their request. If no request is made within thirty days of the request for non-destruction, the recording and the other personal data must be destroyed or deleted. The request shall be submitted to the data protection officer.

(2) Detailed rules on the exercise of the data subject's rights are set out in the other chapters of this Policy.

Chapter VII
Miscellaneous and closing provisions

Article 25

(1) Statements and instructions regarding data processing must be made in writing. Where all the circumstances of the case justify urgent oral communication, statements and instructions made in this way shall be put in writing without delay after the circumstances giving rise to the oral communication have ceased to exist. For internal operations-related matters, statements and instructions sent by e-mail shall always be considered as appropriate and sufficient communication made in writing.

(2) In actions related to data protection, the utmost effort shall be made at all times to ensure that compliance with this Policy and the legal requirements can be demonstrated, in particular with respect to the following:

a) the data subject's consent to the processing;

b) the explicit consent of the data subject to the processing of their sensitive data;

c) the erasure, rectification or confirmation of the fulfilment of the data restriction by the data

subject;

d) the notification of data breaches to data subjects, and

e) data transfers to third countries.

In the above cases, the written form (or the form qualifying as written) shall be used, even in urgent cases, to ensure verifiability. The operational background related to online systems shall be designed to ensure that these needs are met – for example, that the consent to processing given by the identified data subject can be established clearly.

(3) No performance from any third party that contains personal data, the lawful processing of which is not guaranteed by the University or the third party, may be accepted. This provision must be included in all contractual agreements with third parties.

(4) The University's employees and contractors are individually and directly responsible for compliance with data protection rules. The latter shall be liable without limitation for any damage arising in connection with the processing (in particular, for fines imposed by public authorities, aggravated damages (compensation for injury to feelings) paid to the data subject in connection with the processing, and for loss of reputation and loss of profits).

(5) This Policy shall be reviewed by the CEO as necessary, but at least every two years. This Policy shall enter into force on 7 October 2022 and, simultaneously with this, the University's Privacy Policy, which entered into force on 7 December 2018, and the Policy on the Electronic Surveillance System operated on the premises of the Moholy-Nagy University of Art and Design Budapest, which entered into force on 20 July 2020, shall be repealed.

Budapest, 4 October 2022

Zsuzsanna Kun
CEO

Annexes:

Annex 1: Request form – to access data of public interest

Annex 2: Information on the location of cameras

MOHOLY-NAGY
művészeti egyetem
university of art and
design budapest

Annex 1

REQUEST FORM*

To access data of public interest

Name of applicant (name of the natural person, legal person or other entity without legal personality)	
Name of representative (in the case of a legal person or other entity without legal personality, the name of the acting representative)	
Postal address:	
Daytime availability (phone, fax, e-mail)	
Identification of the data of public interest requested:	
Copy of the data (underline as appropriate)	• I request a copy • I do not request a copy
Only to be filled in if you request a copy! Copies made (underline as appropriate)	• I wish to receive them in person • I wish to receive them by post • Please send them in electronic form

I undertake to pay the costs incurred in connection with the preparation of the copies to the Moholy-Nagy University of Art and Design Budapest before the copies are received.

By signing below, I acknowledge that, if the request for access to data of public interest submitted by me needs to be clarified or supplemented in order to be fulfilled and I do not provide the necessary information upon request of the data controller, the data controller shall consider my request as withdrawn.

Budapest, _____ 20__

_____

signature

* After the case is closed, the personal data must be deleted in accordance with Article 10(2) of this Policy.

MOHOLY-NAGY
művészeti egyetem
university of art and
design budapest

Annex 2

Information on the location of cameras

ONE Workshop House

Camera name	building	floor	premise number	premise name	Direction	Angle of view (degrees)
Camera 1: ground floor service entrance	MH	-1st floor	outdoor	entrance	TWO service entrance and external gate on Budakeszi út	120 degrees
Camera 2: basement	MH	-1st floor	P19	lobby	O_-104 staircase door and distribution cabinet	90 degrees
Camera 3: basement	MH	-1st floor	P02	lobby	O_-110 photocell door and staircase side wall towards UP	90 degrees
Camera 5: ground floor staircase entrance	MH	ground floor	002	lobby	O_001 wall elevator and staircase back wall	90 degrees
Camera 7: ground floor staircase	MH	ground floor	002	lobby	O_005 wall stairs and photocell door	90 degrees
Camera 8: outdoor 0 floor	MH	1st floor	outdoor	lobby	in the continuation of the bridge from the outer corner of the building towards building 'A', tegra pavement	120 degrees
Camera 9: 1st floor staircase	MH	1st floor	102	lobby	O_101 from wall towards staircase and elevator	90 degrees
Camera 10: 1st floor staircase	MH	1st floor	102	lobby	O_109 from workshop corner towards staircase back	90 degrees
Camera 11: 2nd floor 1 staircase	MH	2nd floor	202	lobby	O_206 from the wall to the side wall of the staircase towards Up	90 degrees
Camera 12: 2nd floor 1 staircase	MH	2nd floor	202	lobby	O_204 from the wall towards the Master lobby is visible	90 degrees

TWO Studio House

Camera name	building	floor	premise number	premise name	Direction	Angle of view

						(degrees)
Camera 1: 2P passageway	MM	-2nd floor	T_-216	passageway	Overlooking T_-222, under bridge	90 degrees
Camera 2: 2P elevator lobby	MM	-2nd floor	2P02	passageway	Overlooking T_-208, elevator and doors opening from corridor are visible	90 degrees
Camera 3: 1 P elevator lobby	MM	-1st floor	1P02	passageway	Overlooking T_-118, elevator and doors opening from corridor are visible	90 degrees
Camera 5: 1P passageway	MM	-1st floor	T_-118	passageway	Overlooking T_-123, doors opening from corridor are visible	90 degrees
Camera 6: ground floor bridge entrance	MM	ground floor	0008	coffice	photocell entrance door under bridge and T_014 door	90 degrees
Camera 8: ground floor staircase entrance	MM	ground floor	T_010	staircase	from staircase towards the terrace overlooking the emergency exit	90 degrees
Camera 9: ground floor elevator lobby	MM	ground floor	0008	coffice passageway	from service corridor, elevator lobby, row of student lockers, service gateway	90 degrees
Camera 10: ground floor film studio lobby	MM	ground floor	0008	coffice passageway	overlooking the entrance of the film studio lobby, facing the fire hydrant, towards emergency exit route	90 degrees
Camera 11: ground floor cargo passenger entrance	MM	ground floor	T_017	passageway	from coffice, the corridor camera facing the service entrance	90 degrees
Camera 12: ground floor entrance to the props storage	MM	ground floor	T_009	props storage	overlooking props storage cargo entrance and freight elevator downwards	90 degrees
Camera 13: 1st floor bridge entrance	MM	1st floor	0102a	passageway	from the inner end of the space experiment, overlooking the bridge through the photocell door	90 degrees
Camera 14: 1st floor passageway	MM	1st floor	0102a	passageway	looking outwards from the T_105 wall, showing the doors, including the elevator and staircase	90 degrees
Camera 15: 1st floor passageway 2	MM	1st floor	0102a	passageway	facing inwards from the staircase towards T_105	90 degrees
Camera 16: 2nd floor passageway	MM	2nd floor	0202	passageway	facing outwards from the staircase, the elevator and doors opening from the corridor are visible	90 degrees
Camera 17: 2nd floor machine-room	MM	2nd floor	0211	machine room	mechanical space above the film studio, liquid coolers	90 degrees

Camera 18: ground floor buffet	MM	ground floor	0008	coffice	T_011 warehouse from outside corner towards photocell towards buffet and lobby	90 degrees

Master "A"

Camera name	building	floor	premise number	premise name	Direction	Angle of view (degrees)
Camera 1: P Secretariat	Master	-1st floor	MA.-1.02	aula	from the connecting staircase to the door of the secretariat from the outside	90 degrees
Camera 2: P aula	Master	-1st floor	MA.-1.02	aula	to connecting stairs towards the ground	90 degrees
Camera 3: P passageway	Master	-1st floor	MA.-1.11	passageway	from aula towards Base, installed at the aula gateway door	90 degrees
Camera 5: P passageway	Master	-1st floor	MA.-1.12	passageway	overlooking the aula, from the common wall of AB	90 degrees
Camera 6: P gateway	Master	-1st floor	MA.-1.34	A-B gateway	From AB common wall towards the hall	90 degrees
Camera 8: ground floor passageway	Master	ground floor	MA.002	passageway	from aula towards Base, installed at the aula gateway door	90 degrees
Camera 9: 1st floor aula	Master	1st floor	MA.1.02	aula	From M_113 wall towards the staircase and terrace exit, entrance to home space	90 degrees
Camera 10: 1st floor home space	Master	1st floor	M_105	home space	above the entrance door	120 degrees
Camera 11: 1st floor passageway	Master	1st floor	MA.1.16	passageway	fire escape door, home space door, M111 project room door	90 degrees
Camera 12: 2nd floor aula	Master	2nd floor	MA.2.02	aula	auditorium, elevator, stairs, brand office entrance	90 degrees
Camera 13: 2nd floor home space	Master	2nd floor	M_206	home space	above the entrance door	120 degrees
Camera 14: 2nd floor passageway	Master	2nd floor	M.2.17	passageway	M_212 project room door, fire escape, passageway window	90 degrees

Camera 15: 3rd floor campus	Master	3rd floor	M_311	CI lobby	first section, facing entrance door	90 degrees
Camera 16: 3rd floor cash desk	Master	3rd floor	M_313	archives	looking at the SALGO shelves	90 degrees
Camera 17: 3rd floor home space	Master	3rd floor	M_307	home space	above the entrance door	120 degrees
Camera 18: 3rd floor kitchenette	Master	3rd floor	MA3.13	passageway	fire staircase door, M_309 sanitary block passageway door	90 degrees

Base "B"

Camera name	building	floor	premise number	premise name	Direction	Angle of view (degrees)
Camera 1: P elevator lobby	Base	-1st floor	MB_-1.02	elevator lobby	elevator, part of door B_-109	90 degrees
Camera 2: P hall	Base	-1st floor	B_-107	hall	from top right corner of gateway door towards the glass wall, heat centre door	90 degrees
Camera 3: P gateway	Base	-1st floor	AB gateway	gateway	From B wall towards A full corridor	90 degrees
Camera 5: P gateway	Base	-1st floor	AB gateway	gateway	From building 'A' towards 'B', full corridor	90 degrees
Camera 6: ground floor right	Base	ground floor	MB_0.02	elevator lobby	Elevator doors, part of the B_003 cleaning products storage door	90 degrees
Camera 8: ground floor wind shelter structure	Base	ground floor	MB0.01	coffice	overlooking the wind shelter structure towards Master	90 degrees
Camera 9: ground floor left	Base	ground floor	MB0.01	coffice	elevator doors, part of the B_008 cleaning products storage door	90 degrees
Camera 10: 1st floor right	Base	1st floor	MB1.02	passageway	elevator doors, part of the B_105 cleaning products storage door	90 degrees
Camera 11: 1st floor left	Base	1st floor	MB1.02	passageway	elevator doors, part of the B_112 cleaning products storage door	90 degrees
Camera 12: 2nd floor right	Base	2nd floor	MB2.02	passageway	elevator doors, part of the B_203 cleaning products storage door	90 degrees

Camera 13: 2nd floor left	Base	2nd floor	MB2.02	passageway	elevator doors, part of the B_207 cleaning products storage door	90 degrees
Camera 14: 3rd floor right	Base	3rd floor	MB3.02	passageway	elevator doors, part of the B_305 cleaning products storage door and 306 home space right entrance	90 degrees
Camera 15: 3rd floor left	Base	3rd floor	MB3.02	passageway	306 home space left entrance	90 degrees

Chill zone "GV"

Camera name	building	floor	premise number	premise name	Direction	Angle of view (degrees)
Camera 1: P Secretariat	Master	-1st floor	MA.-1.02	aula	from the connecting staircase to the door of the secretariat from the outside	90 degrees
Camera 2: P aula	Master	-1st floor	MA.-1.02	aula	to connecting stairs towards the ground	90 degrees
Camera 3: P passageway	Master	-1st floor	MA.-1.11	passageway	from aula towards Base, installed at the aula gateway door	90 degrees
Camera 5: P passageway	Master	-1st floor	MA.-1.12	passageway	overlooking the aula, from the common wall of AB	90 degrees
Camera 6: P gateway	Master	-1st floor	MA.-1.34	A-B gateway	From AB common wall towards the hall	90 degrees
Camera 8: ground floor passageway	Master	ground floor	MA.002	passageway	from aula towards Base, installed at the aula gateway door	90 degrees
Camera 9: 1st floor aula	Master	1st floor	MA.1.02	aula	From M_113 wall towards the staircase and terrace exit, entrance to home space	90 degrees
Camera 10: 1st floor home space	Master	1st floor	M_105	home space	above the entrance door	120 degrees
Camera 11: 1st floor passageway	Master	1st floor	MA.1.16	passageway	fire escape door, home space door, M111 project room door	90 degrees
Camera 12: 2nd floor aula	Master	2nd floor	MA.2.02	aula	auditorium, elevator, stairs, brand office entrance	90 degrees

Camera 13: 2nd floor home space	Master	2nd floor	M_206	home space	above the entrance door	90 degrees
Camera 14: 2nd floor passageway	Master	2nd floor	M.2.17	passageway	M_212 project room door, fire escape, passageway window	90 degrees
Camera 15: 3rd floor campus	Master	3rd floor	M_311	CI lobby	first section, facing entrance door	90 degrees
Camera 16: 3rd floor cash desk	Master	3rd floor	M_313	archives	looking onto the SALGO shelves	90 degrees
Camera 17: 3rd floor home space	Master	3rd floor	M_307	home space	above the entrance door	90 degrees
Camera 18: 3rd floor kitchenette	Master	3rd floor	MA3.13	passageway	fire staircase door, M_309 sanitary block passageway door	90 degrees
Camera 1: P elevator lobby	Base	-1st floor	MB_-1.02	elevator lobby	elevator, part of door B_-109	90 degrees
Camera 2: P hall	Base	-1st floor	B_-107	hall	from top right corner of gateway door towards the glass wall, heat centre door	90 degrees
Camera 16: Chill zone	GV	ground floor	MGV.0.01	passageway	above main entrance, corridor and back door are visible, overlooking the rest room	90 degrees

UP "TK"

Camera name	building	floor	premise number	premise name	Direction	Angle of view (degrees)
Camera 1: P Secretariat	Master	-1st floor	MA.-1.02	aula	from the connecting staircase to the door of the secretariat from the outside	90 degrees
Camera 2: P aula	Master	-1st floor	MA.-1.02	aula	to connecting stairs towards the ground	90 degrees
Camera 3: P passageway	Master	-1st floor	MA.-1.11	passageway	from aula towards Base, installed at the aula gateway door	90 degrees
Camera 5: P passageway	Master	-1st floor	MA.-1.12	passageway	overlooking the aula, from the common wall of AB	90 degrees
Camera 6: P gateway	Master	-1st floor	MA.-1.34	A-B gateway	From AB common wall towards the hall	90 degrees

Camera 8: ground floor passageway	Master	ground floor	MA.002	passageway	from aula towards Base, installed at the aula gateway door	90 degrees
Camera 1: P elevator lobby	UP	-1st floor	U_-102	passageway	On U_-102 wall, overlooking the elevators and staircase door	90 degrees
Camera 2: ground floor reception	UP	ground floor	TK.017	ground	from the outer corner of the library onto the reception, main entrance and exhibition wall, up to the lower 1/3 of the stairs	120 degrees
Camera 3: ground floor entrance	UP	ground floor	TK0.04	passageway	overlooking the entrance wind shelter structure next to the library, with the passageway to the elevator visible	90 degrees
Camera 5: ground floor main entrance	UP	ground floor	TK.017	ground	main entrance doors with the wind shelter structure from reception	90 degrees
Camera 6: ground floor wind shelter structure	UP	ground floor	TK.044	ground	wind shelter structure interior (partly, 2.5 doors)	90 degrees
Camera 7: ground floor kitchen	UP	ground floor	TK.0.22	kitchen	serving desk and window	90 degrees
Camera 8: ground floor workcentre	UP	ground floor	TK.0.23	passageway	service corridor (printshop doors tangentially)	90 degrees
Camera 9: 1st floor elevator lobby	UP	1st floor	Tk.1.02	elevator lobby	to library, from management offices	90 degrees
Camera 10: 2nd floor wind shelter structure	UP	2nd floor	U201	wind shelter structure	To TK2.03	90 degrees
Camera 11: 2nd floor elevator lobby	UP	2nd floor	TK2.02	passageway	looking towards the elevator from the wind shelter	90 degrees
Camera 12: 3rd floor elevator lobby	UP	3rd floor	TK3.02	passageway	From U301 towards the elevator	90 degrees
Camera 13: 4th floor elevator lobby	UP	4th floor	TK4.02	passageway	elevator from the open passageway, copying kitchenette	90 degrees
Camera 14: 5th floor elevator lobby	UP	5th floor	TK5.02	passageway	From U507 elevator, U520 meeting room, 519 office	90 degrees
Camera 15: 2nd floor material library	UP	2nd floor	U202	material library	Towards the interior of U202	120 degrees