European Media and Immersion Lab

D1.1 – Data Management Plan

WP1 – Management

Authors in Alphabetical Order:

Tuija Heikura (Aalto**)**
Christof Lutteroth (UB)
Tim Moesgen (Aalto)
Juhani Tenhunen (Aalto)
Yu Xiao (Aalto)

Grant Agreement number **101070533**
Action Acronym **EMIL**
Action Title **European Media and Immersion Lab**
Call **HORIZON-CL4-2021-HUMAN-01**

Co-funded by the European Union

UK Research and Innovation

Version date of the Annex I against which the assessment will be made	*Start date of the project*	*Due date of the deliverable*	*Actual date of submission*	*Lead BEN / AP for the deliverable*	*Dissemination level of the deliverable*
18.3.2022	1.9.2022	28.2.2023	28.2.2023	Aalto	PU

Document reviewer(s)	
Name	*Beneficiary*
Christof Lutteroth	UB

Abstract

EMIL has prepared a Data Management Plan (DMP), which describes the data management life cycle for the data to be collected, processed and/or generated by the EMIL project. The DMP will be updated regularly throughout the project (D1.1). Updates of the DMP will be included in the Periodic Reporting Part B.

Contents

1 Introduction and background

This is a living document through the EMIL project lifespan, and it describes the **Initial Data Management Plan (DMP)** for the EMIL project, funded by the EU's Horizon Europe Programme. The purpose of the DMP is to set out the main elements of the EMIL consortium data management policy for the datasets generated by the project. Each EMIL node generates various types of digital data including text and numerical data, images, audio, video, etc. Data is stored in EMIL nodes locally and are available to users according to the user agreement and is backed up according to each organization's guidelines. If devices are taken outside of the premises for data collection, the EMIL facility offers storing of the collected data, and performing data removal from portable devices to protect against unintended data leakage. To guarantee data integrity, data quality is assured with regular calibrations and quality control procedures. The joint data produced if operating EMIL Network interconnected sites is stored in AALTO storage system, the capability of which will be provided by AALTO Science IT infrastructure. Computationally demanding data processing will be facilitated by integrating EMIL storage services with high performance computing (HPC) services provided by each university, and also by both national and European level HPC platforms, such as CSC-RI, and PRACE. As EMIL has a non-EU partner (UB), it should be noted that the U.K. and E.U. have an existing Security of Information Agreement, although this project does not involve any classified information or security issues.

EMIL project gives Financial Support for Third Parties (FSTP) and EMIL partners conduct their own research and development work. Both of these groups generate research related data that can be very sensitive, and both of the groups generate project management (i.e. communication between partners and FSTP beneficiaries and EU) and financial (payments to parties, and internally in partners organisations salaries etc.) related data. We have categorised four different kinds of data the project can generate: 1) the entities' own research and development work will generate both 2) research or development work target group personal data (interviews, sensors' data, video etc.), 3) analysed research data (using for example target group personal data as a source), and 4) the DMP will describe the data management life cycle for the data to be collected, processed and/or generated by EMIL project. As part of making research data findable, accessible, interoperable, and re-usable (FAIR), the EMIL **DMP includes information** on:

- the handling of research data during & after the end of the project
- what data will be collected, processed and/or generated
- which methodology & standards will be applied
- whether data will be shared/made open access and

- how data will be curated & preserved (including after the end of the project).

The data management plan must consider the operating framework, expanded on in Section 4, including intellectual property rights (IPR), the General Data Protection Regulation (GDPR), ethics, the Grant Agreement and Consortium Agreement. The GDPR constrains the handling of personal data and defines the rights of the data subjects.

2 Data types and FAIR data

EMIL has four so-called Lighthouse projects, which may generate various kinds of data, but it also will have FSTP projects, which will start in summer and autumn 2023. FSTP projects can produce very different kinds of data. Lighthouse projects are research and development projects the EMIL partners will execute. FSTP projects are projects by different third-party entities. They are encouraged and helped to open their data according to FAIR data principles whenever possible.

2.1 Data Types of the Project

In the EMIL project we have found four basic types of data (Figure 1): research and development data, analysed research data, project data and reports and communication data.

Research data covers the data collected on the project subject matter, e.g., a new VR or similar systems. The data will be defined more specifically by the Lighthouse projects themselves. The data will be published and stored according to the practices they have used, and also according to the decisions by the EMIL consortium. The research and development data the FSTP projects will generate will be specified in the FSTP project agreements.

Analysed research data refers to qualitative and quantitative data analyses such as reports composed from interviews. Reviews of earlier published data and records will be utilised to some degree. This data will be considered as analysed research data for the purposes of this document. Project related workshops and stakeholder engagement events are public events and the workshop notes of project partners will be treated in the same way as analysed research data (i.e. the notes will be shared within the consortium).

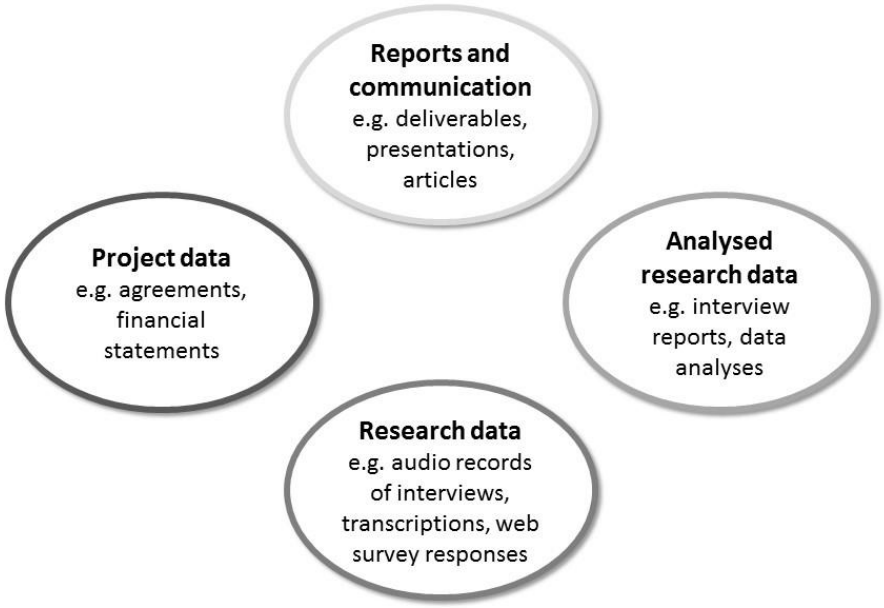

Image 1 Data types.

Project data includes administrative and financial project data, including contracts, partner information and periodic reports, as well as accumulated data on project meetings, teleconferences, and other internal materials. This data is confidential to the project consortium and to the European Commission. Project data includes for example MS Office documents, in English, which ensures ease of access and efficiency for project management and reporting. It also includes financial data. Most of the project data is stored in the password protected Eduuni workspace, administrated by Aalto University.

Reports and other communication data include deliverables, presentations and articles. This data type also includes the contents of the project website.

Each data type is treated differently regarding the level of confidentiality. For example, raw research data such as audios of company interviews are treated as highly confidential data, whereas most project deliverables are actively disseminated. Some of the data falls under the EU and national laws on data protection (GDPR), and for this reason the project is obliged to seek necessary authorisations and to fulfil notification requirements.

The data will partly be in native languages, but all summary documents will be translated to English. The project will assume the principle of using commonly used data formats for the sake of compatibility, efficiency and access. The preferred data types are MS Office compatible formats, where applicable.

2.2 Making data findable, including provisions for metadata

Details on the type of ownerships of the scientific research data are agreed between each partner organization and specific researchers and companies involved in each project. EMIL guidelines will ensure that users will follow existing recommendations issued by the EU on Research Integrity (ALLEA), as well as EU's general data protection regulations (GDPR). EMIL recommends the best licenses according to the level of confidentiality of the data following the principle as open as possible, as closed as necessary.

The EMIL nodes have a remarkable track record of accessible research results in the form of: publications, libraries, datasets and tools. The Lighthouse projects will provide several open SDKs as well as access to the design and implementation of the Smart Garments. EMIL will promote this open access philosophy for the FSTP projects though constraints might apply when they are aimed at direct commercialisation.

EMIL consortium will also take in the account the following questions and making effort to find the best ways to make the data findable and usable for all.

In addition to generic metadata elements, also discipline compliant metadata elements will be used describing the data to aid data discovery and potential re-use, if needed. Persistent identifiers (either DOI or URN) provided by the data repository will be generated and used in linking to datasets.

2.3 Making data openly accessible

The project data (including deliverables, reports, publications, and project's financial data) are open by the default as mentioned in the Projects General Agreement. They are published openly in the EU Funding and Tenders portal according to their level of publicity.

Which data produced and/or used in the project will be made openly available as the default? If certain datasets cannot be shared (or need to be shared under restrictions), explain why, clearly separating legal and contractual reasons from voluntary restrictions.

Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if relevant provisions are made in the consortium agreement and are in line with the reasons for opting out.

How will the data be made accessible (e.g. by deposition in a repository)?

What methods or software tools are needed to access the data?

Is documentation about the software needed to access the data included?

Is it possible to include the relevant software (e.g. in open source code)?

Where will the data and associated metadata, documentation and code be deposited? Preference should be given to certified repositories which support open access where possible.

Have you explored appropriate arrangements with the identified repository?

If there are restrictions on use, how will access be provided?

Is there a need for a data access committee?

Are there well described conditions for access (i.e. a machine readable license)?

How will the identity of the person accessing the data be ascertained?

2.4 Making data interoperable

Are the data produced in the project interoperable, that is allowing data exchange and re-use between researchers, institutions, organisations, countries, etc. (i.e. adhering to standards for formats, as much as possible compliant with available (open) software applications, and in particular facilitating re-combinations with different datasets from different origins)?

The data management will follow and implement a standard format in which the data (and metadata) will be usable across the consortium. This will enable rapid integration for development and benchmark. Variables and value names will be constructed and provided following general data processing conventions common to the research subject. After project closure, metadata of opened datasets will be made available via FAIR compliant repository for research and reuse as described above.

What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?

To promote open science and the wide use of the infrastructure, all efforts to make data openly available, when possible, using services such as Zenodo[1], or fairdata.fi[2], will be assisted or completely handled by EMIL personnel. EMIL encourages good practices of data ownership and user rights to maximize data findability, accessibility, interoperability, and reusage. EMIL personnel will help users with data pseudonymization/anonymization following current state of the art practices (e.g. Finnish Social science Data archive data management guidelines).

[1] https://zenodo.org
[2] https://www.fairdata.fi

In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?

2.5 Openness of the Data – Increase data re-use

Overall, we can define three basic levels of confidentiality, namely Public, Confidential to Consortium (including Commission Services), and Confidential to the Partner or FSTP beneficiary.

1) **Open**: The public data includes reports the deliverables, presentations, and articles. There can be analysed research data too, which may contain some restricted data which can belong to the next category.
2) **Open for the consortium**: Confidential to Consortium (and EU) includes project data (agreements, financial statements etc.). FSTP project proposals will be evaluated by the external Independent Expert Panel (IEP). They will need to sign a confidentiality agreement prior to evaluation (Appendix 1 and 2)
3) **Restricted only for the research unit**: Some parts of the project data can be confidential to the Partner or FSTP Beneficiary. The research data (generated for example in a test by one of the Lighthouses can contain personal data which by default is restricted and must be kept stored according to the GDPR rules or anonymised carefully if published to any other level.

How will the data be licensed to permit the widest re-use possible?

The research data will be collected following jointly agreed guidelines and principles to guarantee the achievement of sound research data and to make the reusability of the research data possible. The project consortium places a strong emphasis on data quality. In all publications also publishing the open research data will follow the conventions found the best in publishing a specific data set. The common practices of setting the data public in the different fields the partners of EMIL and the beneficiaries of FSTP. The EMIL website and EMIL social media channels will be used to maximise the visibility of the deliverables of the project.

When will the data be made available for re-use? If an embargo is sought to give time to publish or seek patents, specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

Are the data produced and/or used in the project useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why.

How long is it intended that the data remains re-usable?

Are data quality assurance processes described?

3 Other research outputs

In addition to the management of data, beneficiaries will consider and plan for the management of other research outputs that may be generated or re-used throughout their projects. Such outputs can be either digital (e.g. software, workflows, protocols, models, etc.) or physical (e.g. new materials, antibodies, reagents, samples, etc.).

Such developer platforms to build, scale and deliver as Github will possibly be used (https://github.com/) .

Beneficiaries should consider which of the questions pertaining to FAIR data above, can apply to the management of other research outputs, and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.

4 Allocation of resources

What are the costs for making data FAIR in your project?

How will these be covered? Note that costs related to open access to research data are eligible as part of the Horizon 2020 grant (if compliant with the Grant Agreement conditions).

Who will be responsible for data management in your project?

Are the resources for long term preservation discussed (costs and potential value, who decides and how what data will be kept and for how long)?

5 Data security

What provisions are in place for data security (including data recovery as well as secure storage and transfer of sensitive data)?

Is the data safely stored in certified repositories for long term preservation and curation?

6 Ethical aspects

Are there any ethical or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

Is informed consent for data sharing and long term preservation included in questionnaires dealing with personal data?

7 Other issues

Do you make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones?

8 Further support in developing our DMP

The Research Data Alliance provides a Metadata Standards Directory that can be searched for discipline-specific standards and associated tools.

The EUDAT B2SHARE tool includes a built-in license wizard that facilitates the selection of an adequate license for research data.

Useful listings of repositories include:

Registry of Research Data Repositories

Some repositories like Zenodo, an OpenAIRE and CERN collaboration, allow researchers to deposit both publications and data, while providing tools to link them.

Other useful tools include DMP online.

Appendix 1

Confidentiality, Conflict of Interest Declaration and Data Processing Agreement

I the undersigned, in participating as an EMIL Independent Expert Panel member in the evaluation of proposals received in the open call of project entitled European Media and Immersion Lab EMIL, declare the following:

Confidentiality and conflict of interest declaration

I undertake to treat as confidential all information contained in the proposals which I am asked to evaluate, both during the evaluation and afterwards.

I will not reveal to any third party the identity or any details of the views of my fellow evaluator(s), neither during the evaluation nor afterwards

I do not, to the best of my knowledge, have any interest in any of the proposals submitted in this call, I have not been involved in their preparation and I do not benefit either directly or indirectly from the eventual selection. Should I discover a conflict of interest during the evaluation, I undertake to declare this and to withdraw from the evaluation.

Data Processing Appendix (DPA)

1. The undersigned independent expert is a personal data processor (later Processor) as defined in the General Data Protection Regulation (later GDPR). The EMIL Consortium Coordinator Aalto University is the designated contact point for the questions related to this processing and the consortium members Aalto University, Filmakademie Baden-Württemberg, Universitat Pompeu Fabra and University of Bath are joint controllers of personal data (later Controller). This DPA is a legal act, that is binding on the Processor, as defined in Article 28 of GDPR.

2. Purpose of the Processing: Processing of personal data in the context of the undersigned acting as a member of Independent Experts Panel and evaluating the proposals for funding submitted by applicants.

3. Nature of the processing: EMIL project application review

4. Types of personal data and categories of data subjects whose personal data is processed: Identifying, contact data and professional data of employees of the companies applying for financial support and of joint controller employees.

5. The Processor shall only process personal data in accordance with the following instructions of the Controller:

- Processor shall process the personal data only for the specific purpose set out in clause 2
- Processor undertakes to securely delete all data related to the proposals after termination of the Purpose, and at the latest at the end of the EMIL project 28.2.2025.
- Processor shall take all measures set out in Article 32 of GDPR and implement appropriate technical and organisational measures so that processing meets the requirements of GDPR and ensures the protection of the data subjects' rights.
- Processor shall notify Controller of all requests of data subjects concerning the exercising of data subject's rights under data protection laws and assist in the fulfilment of these rights.
- Processor shall not use subcontractors in the processing of personal data without the prior written consent from the Controller.
- Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of GDPR and assist Controller in completing all necessary audits.
- If Processor observes any data breach or incident threatening the confidentiality of Personal Data in its possession, Processor will immediately contact Tuija Heikura tuija.heikura(at)aalto.fi and provide all necessary information needed by Controller.
- Processor shall be liable for the damage caused by processing where it has not complied with GDPR or has acted outside or contrary to instructions of the Controller.
- If Processor is located outside EU/EEA in a country without the Commission Adequacy Decision, the Processor will adhere to and sign standard data protection clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

Name		Date	
Signature		Address	

Funded by the European Union

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Appendix 2

EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3972 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[3] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

---

[3] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

EMIL project is funded by the European Union and UK Research and innovation.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the

data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party

located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(f) the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[5].

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 3 months prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which

the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the

categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[6];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent

[6] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Finland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Finland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of Bryssels, Belgium.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

Aalto University Foundation sr

Otakaari 1, Espoo 02150, Finland

Contact person Tuija Heikura, tuija.heikura aalto(at)fi.

Phone: +358 (9) 47001

Data Protection Officer Anni Tuomela dpo(at) aalto.fi

Phone: +358 (9) 47001

Filmakademie Baden-Württemberg GmbH

Animationsinstitut

Akademiehof 10

71638 Ludwigsburg

Phone: +49 7141 969 0

E-Mail: info(at)filmakademie.de

Data Protection Officer for Filmakademie Baden-Württemberg Mr Stephan Hartinger

Coseco GmbH

Telefon: +49 8232 80988-70

E-Mail: datenschutz(at)coseco.de

Universitat Pompeu Fabra, Carrer de la Merce 10-12, Barcelona 08002, Spain

Contact person Narcís Parés Burguès narcis.pares (at)upf.edu

Data Protection Officer dpo(at)upf.edu

University of Bath, Claverton Down, Bath BA2 7AY, United Kingdom,

Contact person Christof Lutteroth cl2073(at)bath.ac.uk

Data Protection Officer Mr D.J. Jolly, djj20(at)bath.ac.uk

Activities relevant to the data transferred under these Clauses: Review of applications for financial support to third parties in The EMIL Project.

Role: Joint controllers

Data importer:

Name: …

Address: …

Position and contact details: …

Member of the Independent Expert Panel of the EMIL Project

Activities relevant to the data transferred under these Clauses: Review of applications for financial support to third parties in The EMIL Project.

*Signature and date:*_____

Role: Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Employees of companies applying for financial support and employees of joint controllers

Categories of personal data transferred

Personal data of employees of the companies applying for financial support: identifying, contact data and professional data (professional category, job, and data related with research projects and activities)

and personal data of joint controller employees: identifying, contact data, and professional data (professional category and job)

Sensitive data transfed

There should not be sensitive data included in the transfer.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

One off transfer for review of EMIL project applications for financial support

Nature of the processing

EMIL project application review

Purpose(s) of the data transfer and further processing

EMIL project application review

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Duration of the review process, latest end of the EMIL Project 28.2.2025. Data must be deleted after the review process. latest at the end of the EMIL Project 28.2.2025.

For transfers to subprocessors, also specify subject matter, nature and duration of the processing

No transfer for subprocessors is allowed.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

The competent supervisory authority in accordance with Clause 13

Data Protection Ombudsman's Office of Finland Home | Data Protection Ombudsman's Office (tietosuoja.fi).

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

- Processor undertakes to securely delete all data related to the proposals after termination of the Purpose, and at the latest at the end of the EMIL project 28.2.2025.
- Processor shall take all measures needed for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services and ensuresthe protection of the data subjects' rights.
- Processor shall take measures for ensuring physical security of locations at which personal data are processed
- Processor shall notify Controller of all requests of data subjects concerning the exercising of data subject's rights under data protection laws and assist in the fulfilment of these rights.
- Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of GDPR and assist Controller in completing all necessary audits.
- If Processor observes any data breach or incident threatening the confidentiality of Personal Data in its possession, Processor will immediately contact Tuija Heikura tuija.heikura(at)aalto.fi and provide all necessary information needed by Controller.
- Processor shall be liable for the damage caused by processing where it has not complied with GDPR or has acted outside or contrary to instructions of the Controller.