



eBRAIN-Health

Deliverable report

D2.4. Public catalogue of data sharing agreements

Submission date	December 2023
Authors	Klaudia Kwiatkowska (UNIVIE) Lukas Faymann (UNIVIE) Nikolaus Forgó (UNIVIE) Tima Otu Anwana (UNIVIE) Petra Ritter (CHARITE)
Dissemination level	PU - Public
Public project website	https://ebrain-health.eu/



Table of contents

Table of figures	3
Public Catalogue of data sharing agreement templates – European Commission Standards	
Contractual Clauses	3
Further Attachements.....	3
1. Introduction.....	4
1.1. Purpose of the deliverable.....	4
1.2. Partners involved and work performed.....	4
2. Data sharing agreements	5
2.1. Purpose of data sharing agreements under the GDPR.....	5
2.2. Definitions.....	6
2.3. Data Sharing in eBRAIN-Health	6
3. European Commission Standard Contractual Clauses (SCCs).....	7
3.1. Introduction	7
3.2. Controller-processor SCCs.....	8
3.3. Use case: HCP Young Adult Connectomes data set.....	11
3.3.1. OS Licence for non-personal data.....	11
3.4. Transfer to third countries	12
4. Internal data flow in eBRAIN-Health.....	14
4.1. Introduction.....	14
4.2. Questionnaire.....	14
5. Guidelines for concluding a data sharing agreement using the EC model SCCs	14
5.1. Introduction.....	144
5.2. Determining the role allocation according to the GDPR.....	15
5.3. Information to be provided for each template	17
5.3.1. Controller-Processor SCCs.....	17
5.3.2. SCCs for data transfers to third countries	18
5.4. Internal collection and storage of concluded data sharing agreements	21
6. Conclusion	21
Bibliography.....	22
Annexes	23



Table of figures

Table 1 – Data Providers

Public Catalogue of data sharing agreement templates – European Commission Standards Contractual Clauses

Annex 1 - model EC SCC for international data transfers

Annex 2 - model EC SCC EU-EEA controller-processor

Annex 3 – EN Annex Standard Contractual Clauses EU-EEA-HCP-EBRAINS

Further Attachments

Annex 4 – questionnaire for partners data sharing and internal data flow

Annex 5 - Health Data Cloud General Terms of Use

Annex 6 - Health Data Cloud Privacy Statement



1. Introduction

1.1. Purpose of the deliverable

Data sharing is a crucial aspect of research as it enables to unlock the full potential of data in order to advance knowledge and innovation. Thanks to data sharing, the initial research objectives can be achieved and the reuse of data for various research purposes can be enabled.¹ Data sharing needs to comply with various legal and ethical obligations, including intellectual property and data protection laws. This deliverable focuses on the sharing of personal data, including sensitive data relating to health within the scope of the eBRAIN-Health project. Furthermore, the deliverable aims to provide the consortium partners with tools to successfully conclude data sharing agreements within the scope of the eBRAIN-Health project.

In short, the aim of eBRAIN-Health is to create a platform for studying the human brain and its disorders, such as dementia, in a way that protects personal data. The platform will allow researchers to simulate and model complex brain functions using virtual brains from both healthy individuals and patients. Datasets from different sources will be prepared and organised for analysis. eBRAIN-Health aims to create a new kind of research infrastructure for clinical studies and digital health innovation. It provides an open space for researchers working on dementia and other neurodegenerative conditions while ensuring the protection of sensitive personal data.

In the European Union (hereinafter EU), the General Data Protection Regulation (hereinafter GDPR) sets out rules for the processing of personal data.² The detailed rules regarding data sharing are presented in Sections 2 and 3 of this deliverable.

This deliverable builds on the work conducted so far on the legal and ethical framework of the eBRAIN-Health project. The aim is to offer the eBRAIN-Health consortium partners, researchers from outside the consortium and the general public a tool to gain a deeper understanding of sharing data relating to health for research purposes and the appropriate legal arrangements. In accordance with the FAIR (findability, accessibility, interoperability, and reuse) data principles, this deliverable aims to provide information on how to share personal data in compliance with EU data protection laws.

This deliverable consists of a theoretical part explaining the rationale behind data sharing agreements and the rules applicable in the EU and an introduction to the data sharing workflow in the eBRAIN-Health project. Additionally, the deliverable provides the consortium partners as well as researchers from outside the consortium wishing to use the Health Data Cloud platform³ with guidelines on how to conclude a data sharing agreement based on the Standard Contractual Clauses (hereinafter SCC) provided by the European Commission (hereinafter EC) in order to maintain compliance with the GDPR.

1.2. Partners involved and work performed

This deliverable was prepared by the legal partner, UNIVIE, in consultation and with input by the project coordinator, CHARITE. Other consortium partners, which provide datasets within the project, have been asked for consultation via a questionnaire (Annex 4) on their data sharing practices. This is the list of partners contributing to data sharing or otherwise involved in the sharing of personal data:

¹ <https://www.eurogct.org/research-pathways/public-involvement-and-data/data-sharing-open-data>.

² 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, GDPR) [2016] OJ L 119/1.

³ <https://www.ebrains.eu/health-research-platforms/health-platforms/work-with-health-data-2/>.

**UNIVIE**

- Lead of WP2 (Ethics & Legal)

CHARITÉ

- Project Coordinator & Lead of WP3 (Integration & Technical Coordination)

FRAUNHOFER

- Lead of WP4 (Ontologies & Knowledge Graphs)

FZJ

- Lead of WP5 (Data & Workflows)

OUH

- Lead of WP8 (Big Data Analytics)

UIO

- EBRAINS Curation

INDOC

- Data Platform Development

UCM

- Data Provider

UEDIN

- Data Provider

UNIRM1

- Data Provider

CHUV

- Data Provider

Table 1 - Data Providers

2. Data sharing agreements

2.1. Purpose of data sharing agreements under the GDPR

Data sharing agreements are legal documents that set out the purpose of the data sharing, provide standards and clarify the roles and responsibilities of all parties involved in data sharing. Depending on the relationship and context of data sharing, the GDPR distinguishes the following main types of data sharing agreements:

- Data processing agreement between a controller and a processor (Article 28(3) GDPR),
- Joint controllership agreement (Article 26 GDPR),
- Agreements covering personal data transfers to third countries (Chapter V of the GDPR).

2.2. Definitions



‘Personal data’ is ‘any information relating to an identified or identifiable natural person (**‘data subject’**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.’⁴

‘Sensitive data’ are special categories of data that reveal racial or ‘ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership’ and also genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.⁵

‘Data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.⁶

‘Non-personal data’ means data other than personal data.

‘Processing’ means ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.’⁷ Access to personal data as well as sharing thereof also count as processing.

‘Controller’ According to Article 4(7) GDPR, it is ‘the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.’⁸

‘Joint controllership’ occurs when two or more controllers ‘jointly determine the purposes and means of processing.’⁹

‘Processor’ is ‘a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.’¹⁰

‘Personal data transfer’ is a transfer of personal data from the European Economic Area to a third country.¹¹

‘Standard contractual clauses’ are legal documents, prepared by the European Commission, which may be used to govern the personal data sharing between parties. Contractual clauses may also serve as an appropriate safeguard for data transfers to third countries.¹²

2.3. Data Sharing in eBRAIN-Health

The research infrastructure (hereinafter RI) developed during the eBRAIN-Health project aims to enable data sharing in order to provide researchers with means to develop decision support for dementia with mechanistic insight and predictive power achieved based on multimodal, multi-scale

⁴ GDPR art 4(1).

⁵ GDPR art 9(1).

⁶ GDPR art 4(15).

⁷ GDPR art 4(2).

⁸ GDPR art 4(7).

⁹ GDPR art 26(1).

¹⁰ GDPR art 4(8).

¹¹ E.g. GDPR art 44.

¹² GDPR art 46.



data integration. Brain simulation and machine learning will be used to achieve this goal. In the envisioned user journey, researchers outside of the consortium will be able to request datasets available on the federated Health Data Cloud (hereinafter HDC) platform, upon the conclusion on an appropriate data sharing agreement with the controller and after altering the data to meet the principles of data minimisation in line with the GDPR. Users will be referred – via digital workflows - to the respective data controllers of varying granularity from individual PIs (e.g. in the case of research cohorts), to individual institutions (e.g. in the case of routine hospital data), to national or cross-border entities (e.g. emerging legal acts such as European Health Data Space). The federated approach serves both scenarios, either the code will be transferred to the data not requiring data sharing or data will be shared in a protected dedicated infrastructure after a lawful basis for sharing has been established thereby assigning liabilities to the new data controllers or processors according to the GDPR. eBRAIN-Health will serve a repertoire of solutions tailored to the requirements of a broad range of use cases. Whenever a controller shares data with a processor or third party, it must ensure that the personal data will still be protected in accordance with the rules and principles of the GDPR.

While data sharing will be facilitated by eBRAIN-Health, it will be in full compliance with applicable law and for each use case relevant local data protection officers (hereinafter DPOs) and ethics committees shall be consulted.

All data sharing activities should follow EBRAINS General Terms of Use:

- https://files.ebrains.eu/file/e4b05476-d2f0-49c2-8b45-41f9c317892e/EBRAINS_General_Terms_of_use_e457353c1a_d2122f84c2.pdf

And the Privacy Statement:

- https://files.ebrains.eu/file/e4b05476-d2f0-49c2-8b45-41f9c317892e/EBRAINS_Privacy_Statement_2022_80958229c5.pdf.

Managing personal or health data needs to be done in compliance with Health Data Cloud General terms of Use (see also Annex 5):

- <https://object.hdc.humanbrainproject.eu/public-resources/HDC-Use-Terms-HBP.pdf>

and the Health Data Cloud and Privacy Statement applies (see also Annex 6):

- <https://object.hdc.humanbrainproject.eu/public-resources/HDC-Privacy-Policy.pdf>

3. European Commission Standard Contractual Clauses (SCCs)

3.1. Introduction

On 4 June 2021, the EC issued two sets of modernised standard contractual clauses. The EC adopted these clauses pursuant to two implementing decisions.¹³ There are two sets of ‘pre-approved’ by the EC SCCs – one set for transfers to third countries (Annex 1) and another set for data processing

¹³ Commission Implementing Decision from 4 June 2021 on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, C(2021) 3701 COM; Commission Implementing Decision (EU) 2021/914 of 4 June 2021 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, C/2021/3972.



between a controller and processor (Annex 2).¹⁴ The EC clarifies that the model SCCs are not compulsory and can be used on a voluntary basis in order to comply with GDPR rules.¹⁵

The data sharing agreements concluded with regards to the sharing of datasets on the HDC platform and the eBRAIN-Health project are based on the EC model SCCs. These model SCCs therefore serve as templates and model agreements within the project and for data sharing on the HDC platform. This section explains what the SCCs provided by the Commission consist of and section 4 provides guidelines and explanations on how to fill out the required information.

3.2. Controller-processor SCCs

The purposes of the SCCs for controllers and processors is to help them meet their obligations under Article 28 GDPR. In accordance with Article 28(7) GDPR, the Commission may introduce such SCCs for the matters of constituting a processing agreement between the controller and processor.

Article 28(3) GDPR states that personal data processing by a processor shall be governed by either a contract or another legal act binding under EU or Member State law. This act must be ‘binding on the processor with regard to the controller’ (Article 28(3) GDPR) and set out the ‘subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller’ (Article 28(3) GDPR).

As per Article 28(3) GDPR, the agreement must include that the processor:

- (a) ‘processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) takes all measures required pursuant to Article 32;
- (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III;
- (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
- (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

¹⁴https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

¹⁵ https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en.



- (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.¹⁶

There are three sections in the model SCCs (see also Annex 2) with the minimum required unmodifiable clauses but it is, in principle, allowed for the parties to adopt additional conditions and safeguards as long as they do not contradict the existing clauses or infringe on the fundamental rights and freedoms of individuals.

Section 1

The Clauses in section 1 generally outline the purpose of the SCCs and set rules regarding hierarchy between agreements as well as the invariability and interpretation of the clauses. Additionally, there is a docking clause allowing other parties to enter the Agreement upon completing and signing Annex I of the SCC (Clause 5).

Section 2 – obligations of the parties

The details of processing operations as well as categories of personal data are to be specified in Annex II, section 2 of the model SCCs. Meanwhile, the clauses in section 2 outline the principles of the GDPR, regarding the purpose and storage limitation, security of processing as well as handling of sensitive data (Clause 7). In general terms, the processor must only process data upon the instructions of the controller and for specific purposes agreed upon in the SCCs. Processing may take place only for the duration of a specified period of time. Additionally, when processing sensitive personal data, the processor shall apply ‘specific restrictions and/or additional safeguards.’ (Section 7.5. of Clause 7). The datasets provided in eBRAIN-Health include sensitive data relating to health. Hence, the SCCs concluded between partners and other involved parties should include appropriate restrictions and additional safeguards. For example, the use of encryption and pseudonymisation can be such a tool.¹⁷ Clause 7 also sets out general rules for engaging sub-processors and for international transfers. Clause 8 specifies in what ways the processor shall assist the controller. Among others, the processor shall not respond to any data subject requests prior to obtaining authorisation from the controller. In Clause 9, the obligations regarding notification of data breaches are included.

Section 3 – final provisions

The final section includes clauses on non-compliance by any of the parties and termination of the clauses.

Annexes to the SCCs

Annex I lists the parties to the clauses, identifies the controller(s) and processor(s) as well as, if applicable, their respective data protection officers (hereinafter DPO).

Annex II should contain a detailed description of the processing, including the following:

¹⁶ GDPR art 28(3).

¹⁷ See, for example, European Data Protection Board (EDPB), ‘Secure personal data’ (Data Protection Guide for small business) https://edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en.



- categories of data subjects whose personal data is processed,
- categories of personal data processed,
- 'Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures,'¹⁸
- Nature of processing,
- Purpose(s) for which the personal data is processed on behalf of the controller,
- Duration of the processing,
- For processing by (sub-) processors, also specify subject matter, nature and duration of the processing.

In Annex III, the parties must list the technical and organizational measures, pursuant to Articles 32 GDPR, which the processor must implement.

The following information must be included and 'described concretely – not in a generic manner' (Annex III):

- Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:
 - Measures of pseudonymisation and encryption of personal data
 - Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
 - Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
 - Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
 - Measures for user identification and authorisation
 - Measures for the protection of data during transmission
 - Measures for the protection of data during storage
 - Measures for ensuring physical security of locations at which personal data are processed
 - Measures for ensuring events logging
 - Measures for ensuring system configuration, including default configuration
 - Measures for internal IT and IT security governance and management
 - Measures for certification/assurance of processes and products
 - Measures for ensuring data minimisation
 - Measures for ensuring data quality
 - Measures for ensuring limited data retention
 - Measures for ensuring accountability
 - Measures for allowing data portability and ensuring erasure]
- For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller
- Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

¹⁸ See Annex 2, Annex II.
deliverable report



3.3. Use case: HCP Young Adult Connectomes data set

For the purposes of sharing data in the eBRAIN-Health project and via, in this case, the Virtual Research Environment which is a fully operational node of EBRAINS' Health Data Cloud¹⁹ operated by one of EU's largest University Hospitals and this project's coordinator – the Charité Berlin,²⁰ particularly relevant are the agreements between controllers of datasets and processors. In order to access the data, a data sharing agreement must be concluded between involved parties.

The dataset descriptor Human Connectome Project Young Adult fMRI time series, structural and functional connectomes (v1.0) can be found under this link:

- <https://search.kg.ebrains.eu/instances/88507924-8509-419f-8900-109accf1414b>.

For the purpose sharing this dataset with other entities, such as researchers, a pre-filled data processing agreement (Annex 3) – the EC SCC - was prepared for any potential processors wishing to access the data for their research.²¹ By way of this agreement, the controllers and processors mutually agree on compliance with the GDPR.

Under this link (<https://wiki.ebrains.eu/bin/view/Collabs/hcp-dpa/>) researchers who wish to gain access to this dataset can obtain more information on the data sharing agreement.

This use case serves as an example, how the eBRAIN-Health project and its platform Health Data Cloud facilitate secondary use of sensitive (personal or health) data by:

- 1) Using standardized legal documents for data sharing
- 2) Preparing (pre-filling) and making available sharing agreements for individual data sets containing health or personal information that can be discovered based on their non sensitive meta data, thus facilitating the preparation of such agreements. Only information specific to the secondary data use case, e.g. processing purpose, processor details, data protection measures, need to be added before signing the agreement.
- 3) Provision of a documentation how GDPR compliant processing is achieved within the Health Data Cloud.
- 4) Step-by-step flow diagram showing the requirements for lawful sharing of health and personal data, the fulfilment of which is precondition for providing access to sensitive data for secondary use.

3.3.1.OS Licence for non-personal data

Additionally, the owners of this dataset explicitly allow for the re-use for the non-personal data under the Creative Commons License [Attribution-ShareAlike 4.0 International](https://creativecommons.org/licenses/by-sa/4.0/). It allows the re-use for any non-personal data in this dataset. Among others, it means that this data may be re-used for research.

¹⁹ <https://www.ebrains.eu/health-research-platforms/health-platforms/work-with-health-data-2>

²⁰ The Virtual Research Environment is an extension of the Charité Health Data Platform. On the platform itself, patient data from the Charité hospital is injected and made available for use in research. VRE follows the FAIR data principles. <https://www.bihealth.org/en/translation/network/digital-medicine/bihcharite-virtual-research-environment>.

²¹ <https://wiki.ebrains.eu/bin/view/Collabs/hcp-dpa/>.



For the purpose of making data FAIR (findable, accessible, interoperable, reusable) partners providing datasets in the eBRAIN-Health project are encouraged to allow the reuse of non-personal data via open source licenses, such as [Attribution-ShareAlike 4.0 International](https://creativecommons.org/licenses/by-sa/4.0/).

3.4. Transfer to third countries

The second set of the model EC SCCs aim to serve as a legal basis for international transfers of personal data between a data exporter in the EU and a data importer in a third country. Article 45(1) GDPR requires that personal data only be transferred to third countries which guarantee an adequate level of protection of personal data to the level of protection in the EU. For certain countries, adequacy decisions from the European Commission exist which attest an adequate level of protection. As of December 2023, these are: 'Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay'.²² The GDPR contains other tools for international data transfers, the so-called 'derogations' and other appropriate safeguards under Article 46 GDPR.²³ For the purposes of the eBRAIN-Health project, SCCs are used.

In the case that any of the eBRAIN-Health consortium partners wish to share datasets with entities from outside the EU/EEA as part of the eBRAIN-Health project or through the HDC platform, they need to ensure that there is a legal basis for transferring the data to a third country. If there is no adequacy decision, the model SCCs (Annex 1) may be used. It is a rather complex set of clauses including obligations for all parties to the agreement. In order to guarantee an appropriate level of protection of personal data for data subjects, presently in the eBRAIN-Health project it is foreseen that data sharing with third countries with EC adequacy decisions will also happen using the SCCs for international data transfers.

There are four modules of the model SCCs for international data transfers:

- Module One: controller to controller transfers,
- Module Two: controller to processor transfers,
- Module Three: processor to processor transfers,
- Module Four: processor to controller transfers.²⁴

Section 1

The Sections of the SCCs for international data transfers follow a similar format to the controller-processor SCCs. An important addition is that Clause 3 of section 1 identifies data subjects as third-party beneficiaries who may invoke and enforce several Clauses against both the exporter and importer of the data.

Section 2 – obligations of the parties

Section 2 of the SCCs outlines the obligations of the parties. The data exporter must warrant that they used reasonable effort to ensure that the importer has implemented appropriate technical and

²² https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

²³ GDPR, Chapter V.

²⁴ See Annex 2.



organizational measures to meet the obligations under the SCCs (Clause 8). The importer must comply with general data processing principles. These are specified in Clause 8 and include an obligation to ensure:

- purpose limitation,
- transparency,
- accuracy and data minimisation,
- storage limitation,
- security of processing.

If sensitive data are processed, and this is presumably the case for transfers within the context of eBRAIN-Health, the importer must commit to adopting additional safeguards adapted to the specific nature of the data and the risks involved. Such safeguards may include 'restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure' (Clause 8.6).

Onward transfers, that is further disclosure of the data to other third countries outside the EU/European Economic Area (hereinafter EEA) is forbidden unless the third party receiving the data is also subject to the SCCs or for a limited number of other reasons listed in Clause 8.7.

Parties to the agreement are obliged to demonstrate compliance with its clauses.

Clause 10 includes an obligation to comply with data subject rights and data subject requests. This includes timely compliance with a request for information, access to data or erasure thereof. The ultimate responsibility for this lies with the controller.

Clause 11 obliges the data importer to inform the data subject in a clear and transparent manner on its website about the contact details of a body or person handling complaints. Further clauses outline liability and supervision matters.

The specific clauses vary depending on the transfer module. For instance, in the case of transfers from a controller in the EU to a processor in a third country (Module 2), additional specifications for the security of processing apply (Clause 8.6 of Module Two). Additionally, the importer-processor must erase or return the data once the duration period for processing elapses (Clause 8.5 of Module Two).

Section 3 – local laws and obligations in case of access by public authorities

Section 3 covers the obligations of the parties, particularly the data importer, in instances where local laws may affect compliance with the clauses or access to the data by public authorities.

Section 4 – final provisions

The final provisions can be found in section 4. They cover important procedural matters, such as non-compliance, termination, the governing law and dispute resolution.

Appendix

The Appendix includes important Annexes to the clauses. Details on this part can be found in Section 5.3.2. of this deliverable.



4. Internal data flow in eBRAIN-Health

4.1. Introduction

Mapping out the specific data processing operations and the sharing of data within the eBRAIN-Health project is an ongoing process, requiring consultation with and cooperation between the relevant consortium partners. This task will therefore be continued as the project develops.

4.2. Questionnaire

For the purposes of this deliverable, a questionnaire (Annex 4) has been prepared. This questionnaire aims to map the personal data sharing within the eBRAIN-Health project. Even when sharing personal data between consortium partners, controllers need to conclude an appropriate agreement. The questionnaire collects the following information, which is also useful in preparing a SCC agreement on data sharing:

- Data source and data set(s)
- Dataset(s) controller
- Legal basis for processing personal data
- Legal basis for sharing personal data
- Partner who needs access to dataset during the duration of the project
- Related WP or task
- Legal or other restrictions to the use of the data set(s)
- Information on already concluded data sharing agreements between afore-mentioned partners.

The collected information can also be used to help the respective partners in better understanding the data sharing within the project. It can also be helpful in completing a GDPR-compliant data sharing agreement.

5. Guidelines for concluding a data sharing agreement using the EC model SCCs

5.1. Introduction

This section includes practical guidelines on how to prepare and pre-fill the model SCCs for a controller-processor agreement as well as how to approach SCCs for international data transfers. These guidelines may prove useful for the consortium partners as well as researchers from outside the consortium who wish to access or share data on the HDC platform as well as via the Virtual Research Environment.

Disclaimer: these guidelines are based on legal research by UNIVIE and their application should be made on a case-by-case basis. Partners should always consult their DPO or legal department before concluding a data sharing agreement. UNIVIE disclaims any responsibility for any errors or omissions in the content, or for any actions taken in reliance thereon.



5.2. Determining the role allocation according to the GDPR

The first step to successfully concluding a data sharing agreement is to determine the roles and responsibilities of each party concluding the agreement. The parties need to identify who the controller(s) and processor(s) are.

Controller

Article 4(7) GDPR prescribes that the controller is ‘the **natural or legal person, public authority, agency or other body** which, **alone or jointly with others, determines the purposes and means** of the **processing of personal data**.’²⁵

European Data Protection Board (hereinafter EDPB) Guidelines 07/2020 on the concepts of controller and processor in the GDPR clarify the specific components of this definition.²⁶ As the GDPR places no limitations on who can be a controller, the key is to determine which entity possesses factual control over the purposes and means of processing. It means that this entity exercises ‘decision-making’ power over the processing of personal data.²⁷ Apart from factual influence, in certain cases this control can also stem from an explicit legal competence.²⁸

Only the ‘essential’ means of processing are reserved for the controller. These include means closely connected to the purposes of processing. The EDPB provides the following examples:

- ‘the type of personal data which are processed (“which data shall be processed?”),
- the duration of the processing (“for how long shall they be processed?”),
- the categories of recipients (“who shall have access to them?”),
- and the categories of data subjects (“whose personal data are being processed?”).²⁹

The controller is also the main actor responsible for stipulating and ensuring compliance with measures that ensure security of processing.³⁰

Practical guidelines for controllers:

- Determine who exercises control over the purposes and essential means or processing the data, that is who decides **why** data are processed and **how**,³¹
- Clearly specify the purposes of processing (the ‘**why**’). Additionally, ensure that there is a valid legal basis under Article 6 GDPR (and Article 9 GDPR for sensitive data, including data relating to health),
- Specify the means of processing (the ‘**how**’), focusing on the essential means directly linked to the processing of personal data,

²⁵ GDPR art 4(7).

²⁶ EDPB, ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 2.1)’ (adopted on 07 July 2021), https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf (hereinafter EDPB Guidelines 07/2020).

²⁷ EDPB, Guidelines 07/2020, p. 11.

²⁸ Ibid, p. 11.

²⁹ Ibid, p. 15.

³⁰ GDPR art 5(2), art 32.

³¹ Ibid, p. 14.



- In Annex I of the model SCCs, clearly identify the controller(s) by providing their name, address and contact details – there can be more than one controller.

Joint controllership

It may be that two or more parties jointly exercise a decisive influence over how personal data are processed. Then, the parties are considered joint controllers. As the EDPB explains, ‘an organisation can still be a controller even if it does not make all the decisions as to purposes and means. The criteria for joint controllership and the extent to which two or more actors jointly exercise control may take different forms.’³²

Also in the case of joint controllers, a factual instead of a formal analysis should be carried out as to what kind of control each of the parties exercises over the processing of personal data. The EDPB explains further that the joint participation in the determination of purposes and means of processing can take either form of a common decision or converging decisions from the involved parties.³³

Joint controllers also need to conclude an agreement or arrangement between each other, in accordance with Article 26 GDPR. In such an agreement, they must outline the respective responsibilities concerning the processing of personal data and compliance with the provisions of the GDPR. Joint responsibility does not imply equal responsibility. Rather, joint controllers are accountable for their respective responsibilities.

The joint controllership agreement is a requirement unrelated to any data processing agreement concluded with prospective processor(s).

Practical guidelines:

- If you are in a joint controllership relationship, ensure that there is an appropriate written agreement between the joint controllers. Such an agreement must clearly outline the responsibilities of each controller.

Processor

Article 4(8) GDPR defines the ‘processor’ as a ‘**natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.**’³⁴

Also in this case, there is no limitation as to the type of entity that can be considered a processor. However, it must be an entity separate from the controller. The EDPB provides the following clarification: ‘within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities. On the other hand, a department within a company cannot be a processor to another department within the same entity.’³⁵

A processor only processes data ‘on behalf’ of the controller and acts under the controller’s instructions. Processors do not decide on the purposes of processing but they may have influence on the choice of ‘non-essential’ means of processing. The EDPB explains that a processor should be

³² EDPB, Guidelines 07/2020, p. 14.

³³ Ibid, p. 19.

³⁴ GDPR art 4(8).

³⁵ EDPB Guidelines 07/2020, p. 26.



identified with regards to specific data sets and operations they are instructed to carry out by the controller.³⁶

If a processor processes data for their own purposes, they are considered a controller for this processing and liable under the GDPR.³⁷

The processor has an obligation to assist the controller in implementing technical and organisational measures to ensure the security of processing.³⁸

If a party does not meet the conditions for a processor, it might be that they are considered a third party or a recipient of personal data under the GDPR.³⁹

Practical guidelines for controllers and processors:

- Identify the processor(s) by looking at whether they are a separate entity and process the data in question data solely on behalf of the controller,
- In Annex I of the model SCCs, clearly identify the processor(s) by providing their name, address and contact details – there can be more than one processor,
- As a controller, specify the data sets, data categories and data processing operations in which the processor(s) shall engage,
- As a controller, consider whether the processor(s) may have choice of deciding over ‘non-essential’ means of processing, e.g. the choice of encryption software,
- As a controller, assess whether the processor provides sufficient security measures, e.g. by exchanging relevant documentation or by requesting a risk assessment,⁴⁰
- As a processor, ensure that you continuously provide ‘sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.’⁴¹

5.3. Information to be provided for each template

Each of the two sets of the SCCs require different kind of information to be provided by the parties.

5.3.1. Controller-Processor SCCs

In the above-discussed use case (see Section 3.3. of this deliverable), for Data Processing Agreement for HCP Young Adult Connectomes, the following information is to be provided by the processor in the model SCCs (Annex 2):

- **‘Annex I:**
 - Names and Addresses of all Prospective Processors,

³⁶ Ibid p. 25-26.

³⁷ GDPR art 28(10).

³⁸ GDPR art 32(1).

³⁹ GDPR art 4(9) and 4(10).

⁴⁰ EDPB Guidelines 07/2020, p. 31.

⁴¹ GDPR art 28(1), EDPB Guidelines 07/2020, p. 31.



- Contact information of the responsible institutional Data Protection Officer,
- Signature (either by printing and scanning or with a valid digital signature),
- **Annex II:** Duration of the processing
- **Annex III:** Prospective Processors add to the list of technical and organisational measures carried out to ensure the security of the data, particularly in regard to the safety of the processing after downloading and decrypting the data.⁴²

The pre-filled agreement is included as Annex 3. Prospective processors wishing to access the HCP data set via the Virtual Research Environment are supposed to use this pre-filled agreement.

Practical guidelines for controllers and processors:

- As a (prospective) party to the agreement, ensure that the information provided, such as categories of data subjects and categories of personal data, are as specific as possible,
- When sensitive data, including data relating to health, are to be shared, list any restrictions (also legal) and safeguards applicable to the use and processing of the data,
- The nature and purposes of processing should also be described as specifically as possible, e.g. brain research,
- The duration of the processing should also be provided in specific times frames (from-to),
- The technical and organisational measures specified in Annex 3 should take into account the nature and purposes of processing, e.g. adopt higher security standards for sensitive data relating to health,
- The security measures and information provided should comply with the principles of data processing of Article 5 GDPR and Article 32 GDPR.

5.3.2.SCCs for data transfers to third countries

The following information should be provided for the model SCCs for international data transfers (Annex 1).

Annex I.A.:

- roles of the parties (exporter-importer, controller-processor etc.),
- list of parties including contact details,

Annex I.B.:

- Categories of data subjects whose personal data is transferred,
- Categories of personal data transferred,
- Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures,
- The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis),

⁴² <https://wiki.ebrains.eu/bin/view/Collabs/hcp-dpa/>.



- Nature of the processing,
- Purpose(s) of the data transfer and further processing,
- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period,
- For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.

Annex I.C.:

- Identification of competent supervisory authority.

Annex II must contain a specification of the technical and organisational measures taken by the data importer to ensure security of the processing and a level of protection of personal data essentially equivalent to that in the EU.

Annex II:

- Measures of pseudonymisation and encryption of personal data,
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services,
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing,
- Measures for user identification and authorisation,
- Measures for the protection of data during transmission,
- Measures for the protection of data during storage,
- Measures for ensuring physical security of locations at which personal data are processed,
- Measures for ensuring events logging,
- Measures for ensuring system configuration, including default configuration,
- Measures for internal IT and IT security governance and management,
- Measures for certification/assurance of processes and products,
- Measures for ensuring data minimisation,
- Measures for ensuring data quality,
- Measures for ensuring limited data retention,
- Measures for ensuring accountability,



- Measures for allowing data portability and ensuring erasure.

In the *Schrems II* judgement, the CJEU prescribed that an essentially equivalent level of protection of personal data must be ensured in data transfers to third countries.⁴³ Not all third countries might have the same level of protection of personal data. In order to achieve such a level of protection in practice, the Court prescribed the adoption of supplementary measures.⁴⁴ The EDPB adopted Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.⁴⁵ These Recommendations aim to clarify the measures that data exporters may adopt to securely transfer data.

Practical guidelines for data exporters following the EDPB Recommendations 01/2020:

- Know your transfers: record and map the data transfers operations, including any onward transfers. Assess whether the transfers comply with the data minimisation principle and other general principles of processing,⁴⁶
- Identify what transfer tools you are relying on⁴⁷: check whether there is an adequacy decision by the European Commission for the third country. If you opt for the SCCs, decide which transfer module applies to you by identifying the roles of the parties as in Section 5.2 of this deliverable,
- Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer:⁴⁸ assess, in cooperation with the data importer, whether the third country provides an adequate level of protection. In particular, take into account possible access to the data by public authorities, redress options available for individuals whose data have been accessed etc.⁴⁹ This is a very complex task and requires knowledge of the respective national law systems. Hence, legal departments of the parties to the agreements as well as DPOs should be involved in such an assessment,
- In case of any uncertainties surrounding the level of protection in the third country, as the data exporter you may decide to either suspend the transfer or implement supplementary measures. Supplementary measures proposed by the EDPB include:
 - technical measures (e.g. strong encryption and pseudonymisation)⁵⁰,

⁴³ Case C-311/18, Judgment of the Court (Grand Chamber) of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems (hereinafter Schrems II), ECLI:EU:C:2020:559, paras 96-97.

⁴⁴ Schrems II, para 133.

⁴⁵ EDPB, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) (Adopted on 18 June 2021),

https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (hereinafter EDPB Recommendations 01/2020).

⁴⁶ EDPB Recommendations 01/2020, p. 11

⁴⁷ Ibid, p. 13.

⁴⁸ Ibid, p. 14.

⁴⁹ See also, EDPB, 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures' (Adopted on 10 November 2020),

https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.

⁵⁰ For details, see EDPB Recommendations 01/2020, p. 30-32.



- additional contractual measures (e.g. transparency obligations)⁵¹,
- organisational measures (e.g. transparency and accountability measures, adoption of standards and best practices)⁵²,
- Safeguarding the fundamental rights of individuals as protected by the Charter of Fundamental Rights of the EU, especially the right to privacy (Article 7), right to protection of personal data (Article 8) and right to an effective remedy (Article 47), should remain a priority.⁵³

5.4. Internal collection and storage of concluded data sharing agreements

Data sharing agreements should always be concluded in consultation with legal departments and/or the DPO of the respective parties to the contract.

For the purposes of assessing data sharing in eBRAIN-Health, the concluded data sharing agreements are collected by the coordinator Charite who also operates the EBRAINS GDPR-compliant Health Data Cloud service. Charite takes appropriate measures to store the agreements in a secure environment of its certified critical infrastructure – again in line with GDPR.

After the conclusion of a data processing agreement, the obligations of the controller continue. According to the principle of accountability in Article 5(2) GDPR, the controller must be able to demonstrate compliance with the obligations in the GDPR. In order to comply with that, the controller must collect all the data sharing agreements and store them securely.

6. Conclusion

This deliverable presented the rationale behind concluding data sharing agreements during the eBRAIN-Health project activities and beyond. It offered a theoretical explanation of the types of agreements and roles of different parties in data sharing. Further, for the purpose of this deliverable provided a questionnaire was provided to aid in better understanding one's data sharing operations. Finally, the deliverable includes a catalogue of model data sharing agreements, as prepared by the EC, and offers practical guidelines on how to fill them out in a GDPR-compliant manner. Compliance with data protection laws is one of the main aims of the eBRAIN-Health project. Hence, a commitment to sharing datasets containing personal information in a secure manner is an important aspect of the project. The deliverable serves as a toolkit for consortium partners and researchers to conclude data sharing agreements in the project.

⁵¹ For details, see EDPB Recommendations 01/2020, p. 37-40.

⁵² For details, see EDPB Recommendations 01/2020, p. 41-46.

⁵³ Charter of Fundamental Rights of the European Union [2012] 2012/C 326/02 (CFREU, EU Charter).



Bibliography

Legislation

Charter of Fundamental Rights of the European Union [2012] 2012/C 326/02 (CFREU, EU Charter)

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, GDPR) [2016] OJ L 119/1

Commission Implementing Decision from 4 June 2021 on on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, C(2021) 3701 COM

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 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, C/2021/3972

Guidelines and Recommendations

EDPB, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 2.1)'

EDPB, 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures' (Adopted on 10 November 2020)

EDPB, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) (Adopted on 18 June 2021)

EDPB, 'Secure personal data' (Data Protection Guide for small business) https://edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en

Others

BIH, 'BIH/Charité Virtual Research Environment', <https://www.bihealth.org/en/translation/network/digital-medicine/bihcharite-virtual-research-environment>

EBRAINS, 'Health Data Cloud', <https://www.ebrains.eu/health-research-platforms/health-platforms/work-with-health-data-2/>

EBRAINS, 'General Terms of Use', https://files.ebrains.eu/file/e4b05476-d2f0-49c2-8b45-41f9c317892e/EBRAINS_General_Terms_of_use_e457353c1a_d2122f84c2.pdf

EBRAINS, 'Privacy Statement', https://files.ebrains.eu/file/e4b05476-d2f0-49c2-8b45-41f9c317892e/EBRAINS_Privacy_Statement_2022_80958229c5.pdf



European Commission, 'Standard Contractual Clauses (SCC)',
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

European Commission, 'New Standard Contractual Clauses - Questions and Answers overview',
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en

EURO GCT, 'Data sharing – open data', <https://www.eurogct.org/research-pathways/public-involvement-and-data/data-sharing-open-data>



Annexes



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)¹ 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.

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

¹ 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 [...].

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 ONE: Transfer controller to controller

8.1 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. It may only process the personal data for another purpose:

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

- (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
 - (i) of its identity and contact details;
 - (ii) of the categories of personal data processed;
 - (iii) of the right to obtain a copy of these Clauses;
 - (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
- (b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- (c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.
- (d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

- (a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- (b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- (c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures

to ensure compliance with this obligation, including erasure or anonymisation² of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they 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 subject. 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.
- (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) 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 personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

² This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union³ (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- (i) it 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 of Regulation (EU) 2016/679 with respect to the processing in question;
- (iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

³ 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.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

- (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- (b) The data importer shall make such documentation available to the competent supervisory authority on request.

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 Union⁴ (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.

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.

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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

- (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- (b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
- (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- (d) The data exporter warrants that it has imposed the same data protection obligations on 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 exporter⁵.

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.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union⁶

⁶ 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

(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 of Regulation (EU) 2016/679;
- (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 or the controller 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 controller.
- (c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
- (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- (f) 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.
- (g) 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.

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 purposes of these Clauses.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

- (a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
- (b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
- (c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
- (d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

- (a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data⁷, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
- (c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.

⁷ This includes whether the transfer and further processing 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 or offences.

- (b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

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 [*Specify time period*] 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.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.⁸ The Parties agree that, by complying with this Clause, the data 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 request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. 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

⁸ This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.

MODULE THREE: Transfer processor 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 prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.⁹ The Parties agree that, by complying with this Clause, the data 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

⁹ This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.¹⁰ The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
- (b) In particular, upon request by the data subject the data importer shall, free of charge :
- (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
 - (ii) rectify inaccurate or incomplete data concerning the data subject;
 - (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

¹⁰ That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

- (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
 - (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- (g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

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.

MODULE THREE: Transfer processor to processor

- (a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
- (b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body¹¹ at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor 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.

¹¹ The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

- (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 ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

- (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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.
- (c) 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.
- (d) The Parties agree that if one Party is held liable under paragraph (c), 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.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor 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 ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor 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 ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (*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 safeguards¹²;

¹² 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

- (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 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 ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

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.

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (*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 ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

[OPTION 1: 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 _____ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify country*).

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor 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 _____ (*specify Member State*).

- (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 _____ (*specify country*).

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

.....

Categories of personal data transferred

.....

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.....

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

.....

Nature of the processing

.....

Purpose(s) of the data transfer and further processing

.....

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

.....

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

.....

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

.....

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2. ...



Brussels, 4.6.2021
C(2021) 3701 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 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 (the Clauses) is to ensure compliance with [choose relevant option: OPTION 1: Article 28(3) and (4) 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] / [OPTION 2: Article 29(3) and (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].
- (b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Annex II.
- (d) Annexes I to IV are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- (b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.
- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5 - Optional

Docking clause

- (a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
- (b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
- (c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

- (a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- (b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

- (a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.
- (b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons

authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.
- (d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

- (a) **OPTION 1: PRIOR SPECIFIC AUTHORISATION:** The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned

sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

- (b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- (d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- (e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

- (a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- (b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

- (a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

- (b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions
- (c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
 - (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - (4) the obligations in [OPTION 1] Article 32 Regulation (EU) 2016/679/ [OPTION 2] Articles 33, 36 to 38 Regulation (EU) 2018/1725.
- (d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to [OPTION 1] Article 33(3) Regulation (EU) 2016/679/ [OPTION 2] Article 34(3) Regulation (EU) 2018/1725, shall be stated in the controller's notification, and must at least include:

- (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (2) the likely consequences of the personal data breach;
- (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

- (c) in complying, pursuant to [OPTION 1] Article 34 Regulation (EU) 2016/679 / [OPTION 2] Article 35 Regulation (EU) 2018/1725, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under [OPTION 1] Articles 33 and 34 of Regulation (EU) 2016/679 / [OPTION 2] Articles 34 and 35 of Regulation (EU) 2018/1725.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- (d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller(s): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer*]

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Signature and accession date: ...

2.

...

Processor(s): [*Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer*]

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Signature and accession date: ...

2.

...

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

.....

Categories of personal data processed

.....

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.....

Nature of the processing

.....

Purpose(s) for which the personal data is processed on behalf of the controller

.....

Duration of the processing

.....

.....

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

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

EXPLANATORY NOTE:

The technical and organisational measures need to be described concretely and not in a generic manner.

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

ANNEX IV: LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2. ...



Brussels, 4.6.2021
C(2021) 3701 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 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 (the Clauses) is to ensure compliance with Article 28(3) and (4) 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.
- (b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Annex II.
- (d) Annexes I to IV are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- (b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5 - Optional

Docking clause

- (a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
- (b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
- (c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

- (a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- (b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

- (a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.
- (b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons

authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.
- (d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

- (a) The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.
- (b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

- (c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- (d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- (e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

- (a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- (b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

- (a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
- (b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions
- (c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

- (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
 - (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - (4) the obligations in Article 32 Regulation (EU) 2016/679.
- (d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:
 - (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (2) the likely consequences of the personal data breach;
 - (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

- (c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- (d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller(s):

1. Name: Dr. Michael Schirner

Address: Charité – Universitätsmedizin Berlin, Chariteplatz 1, 10117 Berlin

Contact person's name, position and contact details:

Datenschutz der Charité – Universitätsmedizin Berlin, Charitéplatz 1, 10117 Berlin, +49 30 450 580 016, datenschutzbeauftragte@charite.de

Signature and accession date:

2. Name: Prof. Dr. Petra Ritter

Address: Charité – Universitätsmedizin Berlin, Chariteplatz 1, 10117 Berlin

Contact person's name, position and contact details:

Datenschutz der Charité – Universitätsmedizin Berlin, Charitéplatz 1, 10117 Berlin, +49 30 450 580 016, datenschutzbeauftragte@charite.de

Signature and accession date:

Processor(s):

1. Name:

Address:

Contact person's name, position and contact details:

Signature and accession date:

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

Research Participants

Categories of personal data processed

Health data

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The sensitive data to be processed consists of structural connectomes and functional connectomes of 785 participants of the Human Connectome Project (<http://www.humanconnectomeproject.org/>).

Restrictions/safeguards:

- **Strict purpose limitation:** the data set was minimized to the amount of data that is needed to fulfill the purposes of the processing.
- **Access restrictions:** access is granted to the processor only. The processor may not make the data accessible to anyone else or process the data using systems that allow others to access the data.

Nature of the processing

The data is processed using scientific data analysis techniques involving computational and statistical methods for inspecting, cleansing, transforming and modelling the data.

Purpose(s) for which the personal data is processed on behalf of the controller

Brain research (data subject consent)

Duration of the processing

From to

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

As above

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

- **Encryption:** The data is transferred in encrypted form.
- **Pseudonymization:** The data is pseudonymised: no directly identifying information like names, addresses, dates of births, etc. are contained.
- **Minimization/purpose restriction:** The data is aggregated: the data set does not contain full magnetic resonance imaging recordings of the participants, but only the averaged/aggregated activity in 379 (Glasser Brain Atlas), respectively 84 (Desikan-Killiany Brain Atlas), brain regions.
- **Confidentiality/access control:** The data is processed strictly on confidential computing systems that are protected by access control and regularly updated.
- **Processor:** Processing by a processor is governed by a contract (the standard contractual clauses agreed to in this data processing agreement), that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.
- **Recoverability:** the data can be recovered from the original Human Connectome Project dataset which is publicly available.

Annex 4 – questionnaire on data sharing and internal data flow

WP	WP3	WP4	WP5	WP6	WP7	WP8	WP9
WP leader							
<p>DATA SOURCE AND DATA SETS This refers only to data sets containing personal data (including pseudonymised personal data) which will be uploaded to the HDC or otherwise processed as part of the eBRAIN-Health project.</p>							
<p>DATASET(S) CONTROLLER Indicate the controller (within the meaning of the GDPR) of the datasets, kindly specify whether there is joint controllership and whether appropriate agreements are in place with other joint controllers and/or data processors.</p>							
<p>LEGAL BASIS FOR PROCESSING OF PERSONAL DATA</p>							
<p>LEGAL BASIS FOR DATA SHARING</p>							
<p>PARTNER WHO NEEDS ACCESS TO DATASET DURING THE DURATION OF THE PROJECT If you share or plan to share datasets containing personal data with partners or third parties within the scope of the eBRAIN-Health project, please provide us with information on the scope of the data sharing.</p>							
<p>RELATED WP OR TASK Please provide under which Work Package or task you plan to share the mentioned datasets.</p>							
<p>IS THERE ANY LEGAL RESTRICTION TO THE USE OF THE DATA SET(S)? If there is any restriction, please precise this restriction (legal, regulatory, patent, business model, etc.) E.g. limited to research use only, during and after project, for any purpose. Please indicate the relevant national laws to such a restriction, if applicable.</p>							

DATA SHARING AGREEMENTS Is there any data sharing/licensing agreements in place with a third party to the eBRAIN-Health or a project partner, which sets legal conditions of sharing data (also within the Consortium)? In the affirmative, could you please share such conditions concerning data sharing and the rights granted to you for the further use of such data? If possible, attach the respective DSA/licensing agreement.



HDC General Terms of Use

Version 1.0 (2023 April 28)

Table of Contents

Version History.....	2
1 Scope.....	2
2 Glossary.....	2
3 Accessing the HDC.....	3
3.1 HDC User Account	3
3.2 Personal information we collect	3
3.3 HDC responsibilities	3
4 Transferring Research Data to the HDC	3
5 Accessing Data and Services on the HDC	4
5.1 Limitations of Use.....	4
5.2 Licensing.....	5
5.3 Citation.....	5
6 Intellectual Property	5
7 Other policies and conditions that may apply to you	6
8 Termination and Liability	6
9 Disputes and Disagreements.....	6
10 Contact Us	7
11 Imprint.....	7

Version History

Version	Description	Approval	Date (yyyy-mm-dd)
1.0	Initial General Terms of Use	Petra Ritter	2023-03-03

These General Terms of Use define the relationship between HDC service provider and you as you access and use the Health Data Cloud (HDC). The use of the HDC implies that you accept these terms and conditions. Additional terms of use may apply to the use of specific HDC services.

1 Scope

These terms govern any use of the HDC, including access to content, services, tools, and products available in or through the HDC.

2 Glossary

- **Controller or Data Controller** means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (GDPR Art. 4(7))
- **GDPR** means the General Data Protection Regulation
- **Processor or Data Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (GDPR Art. 4(8))
- **Pseudonymization** means the processing of User’s personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (GDPR Art. 4(5))
- **Technical and Organizational Measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
- **User Account Information** means Personal information about the User for the purpose of providing a User Account on the HDC.
- **User** means a user of the HDC.
- **User’s Data** means data processed by the User via the Services
- **User’s Personal Data** means the personal data contained within the User’s data.
- **Health Data Cloud (HDC)** means the dedicated storage and computing platform provided by the service provider within an IT infrastructure to store and process personal data for research purposes
- **HDC Administrator** means an employee of the service provider or its contracted partners tasked with oversight, operations, and/or maintenance of the HDC.
- **HDC Core** means the data storage zone in which Users can store and process data that has been separated from the uploaded User’s Personal data stored in the Green Room.

- **HDC Green Room** means the data storage zone in which Users can upload and process User's data to pseudonymize and/or limit exposure of potentially sensitive information to those not authorized to view that information.

3 Accessing the HDC

For additional information about how the HDC is accessed and used, please refer to the HDC Access Policy available at <https://object.hdc.humanbrainproject.eu/public-resources/HDC-Access-Policy.pdf>.

3.1 HDC User Account

Access to the HDC requires an HDC user account consisting of a username and password. You certify that the details of your identity provided to the HDC service provider in association with applying for an HDC user account are accurate.

You agree to keep details of your user account, including password, secret. Account credentials are not to be shared with anyone. You must inform HDC support immediately if you suspect any unauthorized use of or access to your password or account (hdc@humanbrainproject.eu)

The HDC service provider and its sub-service providers will not be responsible if you or others suffer any harm or loss because you do not keep your account secure.

3.2 Personal information we collect

When you access or use the HDC, we may collect and process your personal **User Account information**. The type of information collected depends on the services you are accessing or using. The purposes for processing categories of personal data collected and the legal basis for processing can be found in the HDC Privacy Policy available at <https://object.hdc.humanbrainproject.eu/public-resources/HDC-Privacy-Policy.pdf>.

3.3 HDC responsibilities

HDC service provider and its sub-service providers will take appropriate measures to ensure that the processing of your **User Account information** is done in a safe and secure manner and in accordance with applicable data protection law. All requests associated with your rights as a data subject related to user account information collected and processed in the HDC can be made to the Charite Data Protection Officer by emailing: datenschutz@charite.de.

4 Transferring Research Data to the HDC

The HDC allows you to transfer a copy of your research data for the purpose of storing and processing these data in the HDC. The data you transfer to the HDC will be associated with a HDC project. Other HDC users who have been authorized to access this project by a Project Administrator of the project will be able to access all or a subset of the data you transfer to the HDC, and all or a subset of data derived from the data you transfer to the HDC (e.g., the results of any processing conducted on the data you transfer to the HDC).

In transferring data to the HDC, you accept the following terms:

- a) You agree to use the HDC only for the purpose of conducting scientific research or browsing publicly available content for personal interest and not for any other purpose including, without limitation any commercial purpose, without prior written consent of the HDC service provider.
- b) You have the legal authority to transfer and make available data in the HDC for dissemination and use within the HDC.
- c) The data that you transfer to the HDC were collected in compliance with GDPR as well as with ethical, scientific and/or industrial best practices and institutional guidelines.
- d) With respect to data on human subjects or participants, the data you upload to the HDC is limited to data that is necessary for and relevant to the specific purpose of data processing.
- e) You will follow and adhere to the Data Processing Agreement with the HDC service provider for the research project(s) of which you are a member.
- f) With respect to data on human subjects or participants, you will make best efforts to pseudonymize or anonymize such data before you transfer them to the HDC.
- g) If you are required and authorized to transfer identifiable data to the HDC, you will make best efforts to pseudonymize or anonymize the data within the HDC prior to further processing of these data in the HDC.
- h) You will make best efforts to ensure that data you transfer to the HDC does not contain viruses, worms, spyware, malware or any other similar malicious programs.
- i) You will not submit any information or materials into the HDC that infringe or are capable of infringing third party rights, are libellous, obscene, threatening or otherwise unlawful.
- j) You are solely and entirely responsible and liable for the data you transfer to the HDC. You are responsible for the confidentiality of any data processed, downloaded, or copied from the HDC.

The HDC Access Review Committee may at its discretion review your compliance to these terms at any time. Non-compliant data may be removed from the HDC.

5 Accessing Data and Services on the HDC

5.1 Limitations of Use

In using the HDC, you may access the data you have transferred to the HDC, or data shared with you by other HDC users. You may also access HDC features, such as data processing tools, data visualization interfaces, and high performance computing resources.

In accessing such HDC data and features, you agree to the following terms.

- a) When accessing pseudonymized, anonymized or aggregated data on human subjects, you will not attempt to establish the identity of, or attempt to contact any of the data subjects, or perform any unlawful linkage of these data with any other information.
- b) You will not carry out any calculations, operations or transactions that may interrupt, destroy or restrict the functionality of the operation of the HDC or of any program, computer or means of telecommunications.
- c) You will not use the data for high-risk activities such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of HDC features could lead to death, personal injury, or environmental damage.
- d) You may not attempt to gain unauthorized access to HDC data or services, or to the underlying infrastructure, by any illegitimate means. You are required to promptly report any known or suspected illegitimate use or identified weakness to the HDC support team at hdc@humanbrainproject.eu.
- e) You commit to comply with any additional rules and regulations imposed by your institution and your institutional review board in accessing and using data stored in the HDC.
- f) HDC service provider and its sub-service providers make no representations, warranties, or guarantees of any kind to the content or accuracy and quality of the data accessed in or through the HDC. Accessing and using data in the HDC is therefore at your own risk.
- g) HDC service provider and its sub-service providers offer no guarantees regarding reliability, functionality, or availability of HDC features. The HDC platform and/or its systems may be taken off-line at any time for maintenance, upgrades, or other purposes.
- h) HDC is not responsible in the case of loss of data.

5.2 Licensing

Some data and software stored in or provided by the HDC may have explicit licensing conditions. You must follow the licensing conditions required by such data or software, including all restrictions on commercial use, requirements for attribution and requirements to share-alike.

5.3 Citation

If you use content or services from HDC to advance a scientific publication you must follow the applicable citation requirements listed in the data or software licence, or otherwise published by the data or software provider.

6 Intellectual Property

The content, organisation, graphics, design, compilation, magnetic recording, digital conversion and other matters related to the HDC are protected under applicable intellectual property rights (including but not limited to copyrights and trademarks) and other proprietary rights.

Subject to statutory allowances, extracts of material from the HDC may be accessed, downloaded and printed for your personal and non-commercial use except where specified by the licences attached to the HDC resources and services.

7 Other policies and conditions that may apply to you

Further HDC policies and conditions may apply to you and can be found at <https://hdc.humanbrainproject.eu>.

8 Termination and Liability

The data and features available in the HDC are provided on an "as is" and "as available" basis. Please note that HDC features, and content may contain bugs, viruses, errors, problems or other limitations. To the extent permitted by law, HDC service provider and its sub-service providers exclude any warranties (whether expressed or implied) for the HDC platform and data. This includes, but is not limited to, the disclaimer of any implied warranties of merchantability and fitness for a particular purpose of the HDC or of any data stored in the HDC.

Data stored in the HDC may contain advice, opinions, statements or other information by various authors or entities. Reliance upon any such advice, opinion, statement, or other information is at your own risk.

HDC service provider and its sub-service providers disclaim, to the extent permitted by law, all liability and responsibility arising from any use of the HDC or of data stored in the HDC. In particular, but not as a limitation thereof, HDC service provider and its sub-service providers are not liable for any damages (including damages for loss of business, loss of profits, litigation, or the like), whether based on breach of contract, breach of warranty, tort (including negligence), product liability or otherwise, even if advised of the possibility of such damages. The acknowledgment of exclusion of liability is an essential condition for HDC service provider and its sub-service providers in granting access to the HDC and to data stored in the HDC. The HDC and its features and/or data stored in the HDC are provided to users with these limitations only.

HDC service provider and its sub-service providers reserve the right to discontinue at any time, temporarily or permanently, your ability to access the HDC as well as to transfer data to the HDC and/or access data stored in the HDC with or without notice, at its sole discretion and for any reason whatsoever.

HDC service provider and its sub-service providers also take no responsibility for any breach arising from non-compliance with these General Terms of Use by you.

9 Disputes and Disagreements

The substantive laws of Belgium, excluding any conflict of law rules, shall apply to any dispute arising out of the access and use of the HDC pursuant to these General Terms of Use. The ordinary courts of Belgium shall have exclusive jurisdiction, subject to appeal, if any.

This does not affect mandatory legal obligations applicable to you in your jurisdiction.

10 Contact Us

If you have any queries, comments, or concerns about these General Terms of Use, please contact hdc@humanbrainproject.eu

11 Imprint

The HDC is made available and operated by:

<https://www.brainsimulation.org/bsw/zwei/team-contact>



Health Data Cloud (HDC)

Privacy Policy

The Health Data Cloud (HDC) is a computing research infrastructure that is contained within the information technology infrastructure of the Human Brain Project and developed under lead of Charité University Medicine Berlin. The information in this policy is intended to supplement the Data Protection Statement of Charité University Medicine Berlin - which can be accessed at https://www.charite.de/en/service/data_protection/ or by contacting the Data Protection Officer by email: datenschutz@charite.de.

This privacy policy will explain how the HDC uses personal data from two categories of data subjects: (1) users of the platform, and (2) individuals who are participants in research studies whose personal data is processed in the platform as part of a research initiative by an authorized research investigator.

Contents

1	Data Collected from Users of the HDC	2
1.1	What data do we collect?	2
1.2	How do we collect your data?	2
1.3	How will we use your data?	3
1.4	How do we store your data?.....	3
1.5	Marketing.....	4
1.6	What are your data protection rights?	4
2	Data collected from Research Participants	4
2.1	What data do we collect?	5
2.2	How do we collect your data?	5
2.3	How will we use your data?	5
2.4	How do we store your research data?.....	5
2.5	Marketing.....	6
2.6	What are your data protection rights?	6
3	Cookies	7
3.1	What are cookies?	7

3.2	How do we use cookies?.....	7
3.3	What types of cookies do we use?	7
3.4	How to manage cookies.....	7
4	Privacy policies of other websites	8
5	Changes to our privacy policy	8
6	How to contact us	8
6.1	Users of the HDC.....	8
6.2	Research Participants	8
7	How to contact the appropriate authority.....	9
8	Version History	9

1 Data Collected from Users of the HDC

Users of the HDC include members of the public who visit the HDC web portal and registered account holders of the HDC.

1.1 What data do we collect?

The HDC collects the following data from registered account holders:

- Personal identification information such as first and last name, email, and user ID retrieved from EBRAINS IdP.

1.2 How do we collect your data?

Personal user data (first and last name, email, user ID) are obtained from EBRAINS Research Infrastructure (ebrains.eu) where you have registered for a user account. If you are invited to become a member of the HDC it is because you have requested to become a member and an administrator has invited you by email. We collect data and process your data when you:

- Accept an invitation to become a member of HDC and complete the online registration process.
- Complete an application form to become part of the HDC user directory.
- Use or view our website via your browser's cookies.
- Contact HDC support to receive assistance on using the HDC.

1.3 How will we use your data?

The HDC collects your data so that we can:

- Deliver the content of the HDC web portal.
- Provide the research tools and services of the HDC platform.
- Email you with news or maintenance updates about the HDC or to periodically ask for your feedback to continually improve on the features of the HDC.
- Aggregate statistics on platform usage to assist with the operations and future planning needs of the platform.

By applying to create a project on the HDC, and/or by agreeing to the Terms of Use upon registration of your user account, you consent to the collection and use of your data to deliver the services of the HDC.

The HDC may receive support and services from providers outside of the Charité through a contractual relationship. If any personal data is transferred to these providers, the administrator of this website is required to consult the Charité Data Protection Officer to ensure that all data privacy obligations are met.

The legal basis for processing of your personal data by the HDC is your consent, including:

- Your consent to become a member of the HDC and agree to the Privacy Policy (GDPR Art. 6(1)(a))
- Necessity for the performance of a contract to which the Data Subject is a party, or for taking steps at the request of the Data Subject prior to entering a contract (GDPR Art. 6(1)(b)).
- Compliance with a legal obligation (GDPR Art. 6(1)(c)). For example, where the HDC partners are required to store the data to meet bookkeeping or audit obligations.
- Necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR Art. 6(1)(e)).
- If the HDC partners have a legitimate interest that is not overridden by the interests or fundamental rights freedoms of the Data Subject (GDPR Art. 6(1)(f)).

1.4 How do we store your data?

The HDC tools and services are secured within the IT infrastructure of EBRAINS. The HDC will retain your personal information as long as required for the original purpose.

Information stored in log files is periodically erased according to the policies and procedures of the Charité IT department.

Data Subjects may request erasure of their personal data to the Charité Data Protection Officer (DPO). The data controller will execute such requests, except for minimal personal data which may be retained if needed for monitoring legal compliance. Backups may also be retained in case of legitimate interests of the data controller for the continued exploitation of the research infrastructure.

1.5 Marketing

No personal data collected from the HDC website is sold or otherwise shared with third parties for the purposes of direct marketing or other commercial purposes.

1.6 What are your data protection rights?

You have the following rights vis-à-vis the controller (Charité) regarding the processing of your personal data:

The right to access - You have the right to submit a request to the Charité for copies of your personal data.

The right to rectification - You have the right to request that the Charité correct any information you believe is inaccurate. You also have the right to request the Charité to complete information you believe is incomplete.

The right to erasure - You have the right to request that the Charité erase your personal data, under certain conditions.

The right to restrict processing - You have the right to request that the Charité restricts the processing of your personal data, under certain conditions.

The right to object to processing - You have the right to object to the Charité processing of your personal data, under certain conditions.

The right to data portability - You have the right to request that the Charité transfer the data that we have collected to another organization, or directly to you, under certain conditions.

If you would like to exercise any of these rights, please contact us at our email:

[datenschutz\(at\)charite.de](mailto:datenschutz(at)charite.de)

2 Data collected from Research Participants

If you are a research participant, your personal information is collected by a qualified researcher who has been evaluated and approved by relevant authorities (e.g., research ethics board, data protection authorities) to conduct a research study and use the tools and services of the HDC to store and process the data. The researcher's use of the HDC is detailed in a written Data Processing Agreement which is entered into by the researcher and the Charité before the processing takes place.

2.1 What data do we collect?

The HDC does not collect any data from you, the research participant. The HDC processes your data when qualified researchers use the tools and services of the HDC as a processing environment for their research analyses. The researcher determines the data that is collected from you to fulfil the objectives of their research study.

2.2 How do we collect your data?

The HDC does not collect any data from you, the research participant. You provide your data to a qualified researcher who uses the tools and services of the HDC as a processing environment for their research analyses.

2.3 How will we use your data?

The researcher is the data controller and is the only party that may determine the means and purpose of processing your data. The HDC processes your data on behalf of the researcher, as described in a written Data Processing Agreement entered into by both parties.

Employees of Charité and its qualified subcontractors may access research data stored in the HDC in their performance of duties as system administrators of the HDC. Charité has implemented and will maintain Technical and Organisational Security Measures to restrict access to research data to only those employees who require such access and takes appropriate steps to ensure compliance by its employees, contractors and sub-contractors to the extent applicable to their scope of performance and ensure that all persons authorized to process research data are under an obligation of confidentiality and receive adequate training.

Charité will not access, use, or disclose to any third party any research data except as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order).

2.4 How do we store your research data?

Research data in the HDC is stored within the Information Technology (IT) infrastructure of EBRAINS. The Charité maintains policies and procedures governing data security and storage. The HDC retains data processed on behalf of the researcher as required for the researcher's original purpose.

Information stored in log files is periodically erased according to the policies and procedures of the Charité IT department.

The HDC provides researchers with tools and services to retrieve or delete your data. As a research participant, you may request erasure of your personal data that the researcher collected and stored in the HDC. The researcher (data controller) will execute such requests, except for minimal logging or administrative information about the data files themselves which may be retained if needed for

monitoring legal compliance. Backups may also be retained in case of legitimate interests of the data controller for the continued exploitation of the research infrastructure.

2.5 Marketing

No personal data stored in the HDC is sold or otherwise shared with third parties for the purposes of direct marketing or other commercial purposes.

2.6 What are your data protection rights?

You have the following rights vis-à-vis the controller (researcher) regarding the processing of your personal data:

The right to access - You have the right to request the researcher provides copies of your personal data.

The right to rectification - You have the right to request that the researcher corrects any information you believe is inaccurate. You also have the right to request the researcher to complete information you believe is incomplete.

The right to erasure - You have the right to request that the researcher erase your personal data, under certain conditions.

The right to restrict processing - You have the right to request that the researcher restricts the processing of your personal data, under certain conditions.

The right to object to processing - You have the right to object to the researcher's processing of your personal data, under certain conditions.

The right to data portability - You have the right to request that the researcher transfer the data that they have collected to another organization, or directly to you, under certain conditions.

If you wish to make a request under your data protection rights, you should contact the researcher or Data Protection Officer at the institution of the research study where you participated. This information is usually available on a written informed consent form that you signed when you participated in the study.

If you are unable to reach the researcher or don't have that information, please contact the Data Protection Officer of the Charité at our email: [datenschutz\(at\)charite.de](mailto:datenschutz(at)charite.de)

3 Cookies

3.1 What are cookies?

Cookies are text files placed on your computer when you visit the HDC Portal webpage to collect standard Internet log information and visitor behavior information. When you visit our websites, we may collect information from you automatically through cookies or similar technology.

For further information, visit allaboutcookies.org.

3.2 How do we use cookies?

The HDC Portal uses cookies in a range of ways to improve your experience on the HDC website, including:

Some cookies are functional session cookies which are used to provide the user with the experience of a session: e.g., they track login details, remember user choices and preferences, and in some instances determine site permissions. Other cookies are used to provide statistics: e.g., they provide, in anonymous form, the number of visitors accessing a website, features users access during website visits, and the general location of the user based on IP address.

3.3 What types of cookies do we use?

There are a number of different types of cookies, however, the HDC portal website uses only strictly necessary cookies — these cookies are essential for the proper operation of the website, allowing you to browse the website and use its features such as accessing secure areas of the site. This website protects your privacy by not creating cookies which contain personal data. The following list describes the types of cookies used on the HDC website:

- Access token: An encoded token that is used to mark user's identity and access to services.
- Refresh token: An encoded token that is used to refresh user's session.
- Username: Username of the current user
- Login status: Indicates whether or not a user is logged into the HDC
- Terms of Use Notification: Indicates whether or not a user has acknowledged the applicable Terms of Use and Privacy Policy notifications.

3.4 How to manage cookies

You can set your browser not to accept cookies, and the above website tells you how to remove cookies from your browser. However, in a few cases, some of our website features may not function as a result.

4 Privacy policies of other websites

The HDC Portal website may contain links to other websites. Our privacy policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

5 Changes to our privacy policy

The HDC keeps its privacy policy under regular review and places any updates on this web page. This privacy policy was last updated on April 21, 2023.

6 How to contact us

6.1 Users of the HDC

The Charité is the institution responsible for the HDC Research Infrastructure and is the data controller for the personal information of users on the HDC. If you have any questions about the HDC, the Charité privacy policy, or data we hold on you as a user of the HDC, or if you would like to exercise one of your data protection rights, please contact us.

Email us at: [datenschutz\(at\)charite.de](mailto:datenschutz(at)charite.de)

Call us: +49 30 450 580 016

Or write to us at: Charité – Universitätsmedizin Berlin
Charitéplatz 1
10117 Berlin
Deutschland

6.2 Research Participants

The researcher who collected your data is the data controller for the personal information you provided for research purposes. If you have any questions about your participation in the research study and the research data stored about you in the HDC, or you would like to exercise one of your data protection rights, please contact the researcher who collected your data or the Data Protection Officer (DPO) of the institution where your research data were collected.

If you are unable to reach the researcher or don't have this information available, or you have general questions about how your data are processed within the HDC, you may contact the Data Protection Officer (DPO) of the Charité.

Email us at: [datenschutz\(at\)charite.de](mailto:datenschutz(at)charite.de)



Call us: +49 30 450 580 016

Or write to us at: Charité – Universitätsmedizin Berlin
Charitéplatz 1
10117 Berlin
Deutschland

Datasets considered “open for public sharing” that have been processed by researchers in the HDC are posted on the HDC website. If you are a participant in one of these “open for public sharing” datasets and you have questions about the processing of your data in the HDC, you may contact the Charité DPO at the contact listed above.

7 How to contact the appropriate authority

The HDC, its service providers, and the Charité DPO will make every reasonable effort to address your data protection concerns. However, you have a right to lodge a complaint with a data protection authority.

Contact information for the German Federal Commissioner for Data Protection and Freedom of Information is listed below:

Postal address: DerBundesbeauftragten für den Datenschutz und die Informationsfreiheit -
Graurheindorfer Str. 153 - 53117 Bonn

Telephone: +49 (0)228 99 77 99-0

Fax: +49 (0)228 99 77 99-5550

E-mail: poststelle@bfdi.bund.de

Website: <http://www.bfdi.bund.de/>

The competence for complaints is split among different data protection supervisory authorities in Germany.

Competent authorities can be identified according to the list provided under www.bfdi.bund.de/anschriften

Contact information for the European Data Protection Board and EU DPAs is available here: https://edpb.europa.eu/about-edpb/board/members_en

8 Version History

Version	Description	Approval	Date (yyyy-mm-dd)
1.0	Initial Version		

1.1	Remove "Draft" watermark and update version date.		
-----	---	--	--