

# **Agreement for joint personal data controllership**

**Detta dokument är framtaget och kvalitetssäkrat av Kliniska Studier Sverige.**

Vi utvecklar och erbjuder stöd för kliniska studier i hälso- och sjukvården.

Stödet vi erbjuder ger goda förutsättningar för kliniska studier av hög kvalitet.

About the document

Agreement for joint personal data controllership was published 2022-03-21. This is version 1.0.

Agreement for joint personal data controllership

between

[Party A]

and

[Party B]

20YY-MM-DD

Table of Contents

[1. Background and purpose 3](#_Toc112701945)

[2. Definitions and interpretation 3](#_Toc112701946)

[3. Processing of personal data 4](#_Toc112701947)

[4. Ethical review 5](#_Toc112701948)

[5. Rights of the data subjects 5](#_Toc112701949)

[6. Technical and organizational security measures 5](#_Toc112701950)

[7. Data Protection Impact Assessment (DPIA) 6](#_Toc112701951)

[8. Responsible supervisory authority for data protection 6](#_Toc112701952)

[9. Personal data breach 7](#_Toc112701953)

[10. Data processor 7](#_Toc112701954)

[11. Transfers of personal data to a third country or an international organization 7](#_Toc112701955)

[12. Record of processing activities 8](#_Toc112701956)

[13. Costs 8](#_Toc112701957)

[14. Liability 8](#_Toc112701958)

[15. Confidentiality 8](#_Toc112701959)

[16. Arbitration, applicable law 9](#_Toc112701960)

[17. Signatures 10](#_Toc112701961)

[Appendix 1 – Parties to this Agreement 11](#_Toc112701962)

[Appendix 2 – Documentation of the Processing 12](#_Toc112701963)

[Appendix 3 – Management of data subjects' rights 15](#_Toc112701964)

[Appendix 4 – Technical and organizational security measures 17](#_Toc112701965)

[Appendix 5 – Personal data processors 21](#_Toc112701966)

This agreement for joint personal data controllership (“Agreement”) has been entered into between the legal entities documented in Appendix 1, separately Party, and jointly the Parties.

## Background and purpose

* 1. The Parties are sponsor and trial site respectively for a clinical trial, as specified in Appendix 2. The Parties have together within the boundaries of a study protocol decided on the purposes and means of the processing of personal data and are thereby joint controllers of said data.
	2. This agreement, with appendixes, is the Parties means of arraignment in accordance with article 26 GDPR.
	3. This agreement’s purpose is to be a transparent determination of each Parties responsibilities in accordance with Data protection legislation in particular regarding rights of the data subjects and providing information to the data subjects.
	4. This agreement regulates respectively the Parties responsibilities to fulfill the obligations according to Data protection legislation. The agreement does not otherwise impose obligation or rights regarding the clinical trial.

## Definitions and interpretation

* 1. The following terms are defined as follows and are reproduced in this Agreement in capital

”Agreement” means this agreement regarding joint controllers including all appendixes.

”the Processing” means the Processing for which all parties are jointly controllers and is documented in Appendix 2.

”Data protection legislation” means GDPR, according to the definition below, and other applicable Data protection legislation which covers the Processing according to Appendix 2.

”GDPR” means the General Data Protection Regulation (2016/679/EU) of the European Parliament and of the Council of 27 April 2016 to the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing of directive 95/46/EG..

”Impact assessment” means Data protection Impact assessment in accordance with article 35 GDPR.

”SCC” means the Arbitration Institute of Stockholm’s Chamber of Commerce.

”Sponsor” means the Party or the Parties that assumes the Sponsor role for the clinical trial.

* 1. Concepts defined in the GDPR shall have the same meaning within this Agreement.
	2. Concepts in section 4 below shall have the same meaning as in the Swedish law (2003:460) on ethical review in research on human beings.
	3. If this Agreement is an Appendix to another contract between the Parties, this section 2 shall take precedence with regards to the definitions of concepts.
	4. In this Agreement the following shall apply:
		1. references to appendixes, sections and paragraphs shall be references to the annexes, sections and paragraphs of this Agreement;
		2. the Appendixes is considered an integral part of the Agreement;
		3. singular includes plural and vice versa, and;
		4. headings shall not influence interpretation of the Agreement.
	5. No part of this agreement shall be interpreted to the disadvantage of a Party by reason of that Party was responsible for drafting the Agreement.

## Processing of personal data

* 1. The Parties are joint controllers for the processing of personal data documented in Appendix 2.
	2. The Parties understands that they are jointly responsible for compliance with all obligations which concerns data controllers under the GDPR. Each Party shall ensure appropriate technical and organizational measures to demonstrate that the Processing is performed in accordance with the GDPR.
	3. The Parties agrees that the joint purpose for the Processing, as documented in Appendix 2, is a scientific research purpose in accordance with the GDPR, unless otherwise is expressly documented in Appendix 2.
	4. The Parties agrees that any processing for another purpose than the one documented in Appendix 2 shall be considered a separate processing and the Party or Parties, which decides the purposes and means for the new processing is considered controller.
	5. The Parties agrees that if a Party is a Swedish public authority, this Party is considered controller, solely not jointly, for any processing which is necessary to uphold the Freedom of the Press Act (1949:105) and the Public Access to Information and Secrecy Act (2009:400).

The Parties understands that a Swedish public authority, according to said acts, independently shall assess if a processing according to this section 3.5 is compliant with Data protection legislation.

The Parties agrees to that one Party’s processing of personal data in accordance with this section, 3.5, is not to be considered a breach of this Agreement.

* 1. The Parties agree that the processing of personal data which a caregiver conducts in accordance with the Swedish Patient data act (2008:355) falls outside the scope of this Agreement. The Parties agree that such a processing is not to be considered a breach of this Agreement.
	2. Since the Parties are joint controllers, any amendment to the Processing regulated in this Agreement demands the written approval of all Parties.

## Ethical review

* 1. The Processing postulates a prior approval from an Ethical Review Authority and that the Study Subject has given informed consent regarding their participation in the research.
	2. In avoidance of any misunderstanding, this Agreement does not regulate the Parties responsibilities regarding scientific or ethical questions.

## Rights of the data subjects

* 1. The Parties understand that a data subject has the right, according to the GDPR, to exercise his rights directly towards each of the Parties. Notwithstanding this, Appendix 3 describes the division that the parties choose to make among themselves as to whom has the main practical responsibility for handling the data subjects’ rights.
	2. The Parties may designate a common point of contact for the purpose of facilitating the data subjects’ rights. If a Party has been designated as a common point of contact, this shall be documented in Appendix 3
	3. Each Party shall ensure that the data subject is informed of the Processing in connection with the data subject giving his or her informed consent to participate in the research, or at the latest before the processing of the data subjects personal data in accordance with this Agreement begins.
	4. Each Party shall ensure that there is documented proof of a data subject having been informed and what that information has been comprised of.
	5. Data subjects have the right to access the essential content of this Agreement. The Parties agree that this right shall be addressed while taking account of each Parties mutual duty of confidentiality in accordance with Section 15 below.

## Technical and organizational security measures

* 1. Taking into account the state of the art, the nature, scope, context and purposes of processing as well as the risk of varying degrees of likelihood and severity for the rights and freedoms of natural persons, each Party shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, and be able to show that the Processing is taking place in accordance with GDPR and Data protection legislation. These measures shall be reviewed and updated at least once (1) a year.
	2. Since the Processing takes place for a scientific research purpose, special requirements are placed on the protection of the data subject’s rights and freedoms. The safeguard measures shall ensure that technical and organizational measures have been put in place to ensure that the principle of data minimization in particular, is observed. These measures shall include pseudonymization, provided that the common purpose for the Processing set out in Appendix 2 can be fulfilled in that way.
	3. The Parties agree that special categories of personal data and national identification numbers are processed and that this places specific demands on technical and organizational measures.
	4. Considering this Section 6, each Party shall comply with the technical and organizational security measures documented in Appendix 4. Nothing in this Agreement shall be interpreted as an impediment for a Party to impose any further technical or organizational measures if appropriate, given the risks, of varying degrees of likelihood and severity, for the rights and freedoms of natural persons.

## Data Protection Impact Assessment (DPIA)

* 1. Before starting the Processing, the Parties shall jointly make an assessment whether a DPIA shall be carried out regarding the Processing. The Parties shall pay particular attention to national decisions on when a DPIA is to be carried out. A DPIA shall always be carried out if a Party so requests. A decision not to carry out a DPIA shall be agreed between the Parties and shall be documented in writing.
	2. The Parties Data Protection Officers shall, in particular within the framework of this Section 7, be given the opportunity to (i) issue an opinion on whether or not to carry out a DPIA, (ii) monitor the process of a DPIA; (iii) issue a statement whether the Data Protection Officer agrees with the conclusions of the DPIA, and (iv) whether the Parties shall conduct a prior consultation.
	3. A DPIA regarding the Processing shall be carried out by one of the Parties. Other parties shall assist this Party with information and advice for the implementation of the DPIA.
	4. A DPIA shall be approved in writing by the other Parties. The Parties thereby also decide whether the DPIA shall result in a prior consultation with the supervisory authority in accordance with the GDPR.
	5. A DPIA, if the Parties decides to implement it, shall without exception be completed before the Processing begins.

## Responsible supervisory authority for data protection

* 1. Since all Parties do not have their principal place of business in Sweden. The Parties common interpretation is that [SWEDEN´s] supervisory authority for data protection is the responsible supervisory authority for the Processing.

## Personal data breach

* 1. The Parties understand that, within the framework of the Processing, they are jointly responsible for complying with obligations under the GDPR regarding notification of a personal data incident to a competent supervisory authority and regarding informing data subjects about a personal data breach.
	2. A Party shall immediately inform the other Parties if the Party has become aware of a personal data breach or suspects that a personal data breach has occurred. This obligation to inform other Parties immediately also applies outside office hours and during public holidays.
	3. A personal data breach shall be reported to the competent supervisory authority, in accordance with this section 9, without undue delay and, not later than seventy-two (72) hours after a Party became aware of the personal data breach, unless the personal data incident is unlikely to pose a risk to the rights and freedoms of natural persons.
	4. In order to avoid misunderstandings, each Party shall, in accordance with Appendix 4, apply appropriate technical and organizational security measures to reduce the risk of personal data breaches.
	5. The Parties shall keep a joint list of established or suspected personal data incidents.

## Data processor

* 1. A Party may assign a data processor to process personal data within the framework of this Agreement only with the written consent of all Parties. A data processor documented in Appendix 5 shall be deemed to have been engaged with the written consent of all parties in accordance with the first sentence of this section
	2. Before hiring a data processor, that Party shall ensure that the processor can provide sufficient guarantees of implementing adequate technical and organizational measures to ensure that the processing meets the requirements of the GDPR and this Agreement and ensure that the data subjects’ rights are protected. In accordance with this, that Party shall carry out a risk assessment to ensure that the data processor’s guarantees are sufficient.
	3. A Party is liable to the other Parties for the content of the agreement or legal act (personal data processing agreement), signed with a data processor, fulfilling requirements set in the Data Protection Legislation and in this Agreement.

## Transfers of personal data to a third country or an international organization

* 1. Unless it is expressly documented in Appendix 2 that the Processing includes the transfer of personal data to a third country or an international organization, according to GDPR Chapter V, the Party transferring personal data to a third country or an international organization is solely controller, individually and not jointly, for any such transfer.

## Record of processing activities

* 1. Each Party shall maintain a record of processing activities in accordance with Article 30 GDPR (Record of processing activities) which includes the joint processing.

## Costs

* 1. Within the framework of this Agreement, each Party shall bear its own costs, unless otherwise expressly agreed between the Parties.

## Liability

* 1. The parties agrees that they are jointly and severally liable for damages in relation to the data subject. Nothing in this Agreement shall be construed as restricting the data subject’s right to indemnity under the Data Protection Legislation.
	2. The parties have an obligation on the basis of this Agreement to limit damage to another Party. Considering this, the Party shall without delay inform the other Parties immediately of such dam<<<age or the risk of such damage.
	3. In light of the Party’s responsibility to demonstrate compliance with the basic principles for the processing of personal data, the Party shall ensure that it has documentation demonstrating accountability and that this Agreement is complied with. For the avoidance of misunderstanding: A party’s inability to demonstrate accountability under Article 5 (2) of the GDPR shall be deemed to be a breach of the Party’s obligation under this Agreement.

*Model clause for liability between the Parties (one shall be selected)*

* 1. If a Party, on the basis of non-compliance with this Agreement, has caused damage to another Party, the party causing the damage shall indemnify the injured Party.
	2. If a Party, on the basis of negligence or fault, caused another Party damage, the causing party shall indemnify the injured party.

## Confidentiality

* 1. According to the GDPR, the data subject has the right to take part of the essential content of this Agreement. The Parties agree that information in Sections 6, 14, and 16, as well as Appendix 4 to this Agreement shall be subject to the Parties mutual duty of confidentiality and may not be disclosed to a data subject or a third party without the consent of all Parties.
	2. To avoid misunderstanding, the Party’s duty of confidentiality under this section 15 does not apply in relation to the national data protection supervisory authority, insofar as this duty of confidentiality would prevent a Party from cooperating with the supervisory authority in accordance with the obligation in Data Protection Legislation.
	3. The parties agree that if a Party is a public Swedish authority, this Party is covered by the principle of public access to information, which affects the scope for confidentiality according to this section to apply only to confidentiality that follows from the Swedish Public Access and Secrecy Act (2009: 400).

## Arbitration, applicable law

* 1. This Agreement supersedes all prior agreements, whether oral or written, between the Parties, regarding the subject matter of this agreement.
	2. The Parties agree that the Swedish law (1980:1102) regarding trading companies and simple companies is not applicable in this agreement.
	3. This Agreement shall be interpreted in accordance with [Swedish law].

To avoid misunderstanding, this does not regulate what Data Protection Legislation should be applicable.

* 1. Disputes arising in connection with this agreement shall be finally settled through arbitration proceedings administered by the Stockholm Chamber of Commerce’s Arbitration Institute (SCC). Rules for Simplified Arbitration shall be applied unless the SCC, taking into account the severity of the case, the value of the subject matter of the dispute and other circumstances, decides that Arbitration Rules shall be applied. In the latter case, the SCC shall also decide whether the arbitral tribunal shall consist of one (1) or three (3) arbitrators.
	2. The seat of the arbitration shall be [Malmö, Sweden].
	3. The language of the arbitration shall be English.
	4. This agreement has been electronically signed by each party.

## Signatures

### **[Party A]**

Signature:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place, date and year

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### **[Party B]**

Signature:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place, date, and year:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Appendix 1 – Parties to this Agreement

This Agreement have been entered by the following Parties:

### [Part A]

|  |  |
| --- | --- |
| Firm: |  |
| Organizational number: |  |
| Seat: |  |
| Postal address: |  |
| Main establishment according to article 4.16 GDPR: |  |
| Representative according to article 27 GDPR, if applicable: |  |
| The Party´s role within the framework of the (i) Processing, and the (ii) clinical trial. |  |

### [Part B]

|  |  |
| --- | --- |
| Firm: |  |
| Organizational number: |  |
| Seat: |  |
| Postal address: |  |
| Main establishment according to article 4.16 GDPR: |  |
| Representative according to article 27 GDPR, if applicable: |  |
| The Party´s role within the framework of the (i) Processing, and the (ii) clinical trial. |  |

## Appendix 2 – Documentation of the Processing

|  |  |
| --- | --- |
| 1. The purpose or purposes of the joint processing:
* *The specific reasons for why the personal data is processed.*
 | The purpose of the personal data processing is […… *for instance to conduct research in accordance with the project’s ethical review decision.]* |
| 1. Description of the processing that occurs in conjunction with the joint controllership:
* *What is actually being done with the personal data?*
 | The processing of personal data consists of: […*these have been collected in conjunction with …]**Here it should be stated what the processing consists of: Normally this refers to the collection of research data, processing of research data, analysis of research data.* |
| 1. Legal basis of the respective parties for the processing of personal data, and, if applicable, for which processing measure or measures the legal basis applies
* *The legal basis according to article 6 GDPR on which each of the parties process personal data.*
 | The legal basis for processing personal data[*… .* *within the framework of the research project is that the processing is necessary to perform a task of public interest in accordance with Article 6 § e) GDPR]**The legal basis for each party should be stated here. In most cases, the legal basis should be that they perform a task of public interest. The public interest is partly based on the organization’s given task of conducting research (in the form of legislation regarding higher education institutions and health providers) and this assignment is also confirmed by the ethics review authority’s decision to allow*  |
| 1. Types of personal data:
* *What kind of categories of personal data that will be processed.*
 | *The types of personal data that occur should be described here, as examples can be mentioned** *Basic contact information like name, address, phone number and e-mail.*
* *Social security number.*
* *Pictures of recognizable individuals.*
* *Personal data regarding relatives/next of kin.*
* *Information from medical records.*
 |
| 1. Categories of sensitive personal data:
* *What kind of categories of sensitive (special) personal data is being processed? There are a specific number of categories listed in article 9.1 GDPR that are considered sensitive.*
 | *Any types of sensitive personal data that is being processed should be described here. (according to article 9.1 GDPR).* *These categories are processed:** *Ethnic origin.*
* *Political opinions.*
* *Religious or philosophical beliefs.*
* *Trade union membership.*
* *Data concerning health.*
* *A natural person’s sex life or sexual orientation.*
* *genetic data.*
* *biometric data for the purpose of uniquely identifying a natural person.*
 |
| 1. Privacy-sensitive personal data, which is not considered sensitive (special) personal data according to article 9.1 GDPR:
* *Any categories that are not sensitive according to the GDPR but are still particularly privacy sensitive and thus may need to be protected.*
 | *It must be stated here whether personal data are included that do not fall into the category of sensitive personal data according to Article 9 (1) GDPR, but are still considered to be particularly worthy of protection.**For example:* * *valuing personal data, such as e.g. grades or other graded assessment.*
* *information about a person's financial circumstances.*
* *information on opinions, (in addition to political).*
* *social security number.*
 |
| 1. Types of data subjects:
* *The categories of data subjects which are included.*
 | *The categories of data subjects which are included should be stated here.** *Research subjects*
* *Next of kin/relative*
 |
| 1. Retention and deletion of personal data:
* *Description of the routines and guidelines that exist regarding how long the personal data will be retained after the project is completed.*
 | When the research project is completed, the personal data will be handled as follows:*[…..in what way they will be preserved and if so how long or when they will be deleted. Such deletion can be achieved either by erasing the personal data or completely de-identifying the same.]* |

## Appendix 3 – Management of data subjects' rights

### Contact point for data subjects

* 1. The Parties has chosen not to appoint a joint contact point for data subjects’ rights.
	2. The Parties have chosen to appoint [Party #] as a joint contact point for data subjects with the following contact information.

### Data subjects’ rights

* 1. The parties agree that they are jointly and severally liable for the rights of the data subjects. Regardless of this, the parties have chosen to make a division between themselves as follows as to which of the Parties that has the main practical responsibility to handle issues concerning the data subjects' rights.

|  |  |
| --- | --- |
| **Right** | **Division of practical responsibilities between Parties** |
| Ensure that information to data subjects is provided in accordance with Articles 12-14 of the GDPR.This information must be produced in [Swedish]. If this information needs to be translated into another language, the Parties shall instruct an authorized translator to carry out this translation. The parties shall jointly bear the cost of producing the information and any translation of the information.The information shall clearly indicate1. that the Parties are jointly controllers for the Processing of personal data;
2. the respective roles of the Parties in relation to the data subject;
3. if a Party is a joint point of contact regarding the rights of data subjects, and
4. that a data subject has the right to exercise his or her rights over and against each of the Parties
 | *Specify the division, if any, the Parties choose to apply about what Party is to ensure that the information is communicated to the data subjects no later than in connection with the commencement of processing.* |
| Ensure that obtained informed consents are handled in a correct manner and that data subjects have been given sufficient information for consents to be considered given correctly.( consents refer to the consents that the research project must provide in accordance with the Ethics Review Authority's approval) | *Specify the division, if any, of duties between the Parties regarding which of them that shall ensure that consents are obtained and handled correctly.* |
| Ensure that data subjects can exercise their rights according to article 15-18 GDPR* Information and access
* Rectification
* Erasure
* Objection
* Restriction
 | *Specify the division, if any, between the Parties regarding which of them that is responsible for managing the data subjects’ various rights.* |
| Ensure that data subjects can exercise their rights according to article 20 GDPR* Right to data portability
 | *Specify the division, if any, between the Parties regarding which of them that is responsible for managing the data subjects right to data portability.**Note that data portability is a right that is only applicable if the legal basis for the processing is the data subjects’ consent (or necessary for the performance of a contract) neither of which is normally the legal basis for processing personal data within scientific research.* |

## Appendix 4 – Technical and organizational security measures

The parties note that the requirements set out below are a minimum for the current processing of personal data and that these requirements are therefore also applied and fulfilled by all the Parties responsible for personal data.

The respective Parties of the joint personal data controllership confirm by entering into this agreement that in their processing of personal data relevant to the agreement, they apply all of the following technical and organizational security measures and thus comply with Article 32 of the GDPR.

### Management system for information security

* 1. Each Party shall, through a management system, ensure that:
		1. documented personal data of the Party is accessible and useful to the person authorized (*availability*),
		2. personal data is undistorted (*accuracy*),
		3. unauthorized persons shall not be able to access the personal data (*confidentiality*), and;
		4. actions can be traced to a user (*traceability*) in information systems that are fully or partially automated
	2. Each Party shall ensure that an information security policy is in place. The policy shall set out the Parties' overall goals for and the operations work with information security in order to ensure the availability, accuracy, confidentiality and traceability of personal data.
	3. Each Party shall appoint one (1) or more persons to lead and coordinate the information security work.
	4. Each Party shall regularly assess whether there are risks of events that may result in the obligations in this Appendix 4 not being complied with (risk analysis). For each such event, the Party shall (i) estimate the probability of the event occurring, and (ii), assess the negative consequences that would result from the event. The risk analysis must be documented in writing.
	5. In order to avoid misunderstandings: Each Party shall ensure that any personal data processors working for them are subject to obligations regarding technical and organizational measures which materially correspond to this Annex 4

### Availability

#### Backup

* 1. Each Party shall ensure that personal data processed in IT-systems are backed up with a fixed periodicity. The backup copies must be stored securely, well separated from the original information. The Party shall decide on how long the backup copies shall be kept and how often re-reading tests of the copies shall be performed.

#### Continuity planning

* 1. The Party shall plan for how the processing is to be carried out if IT-systems used for the processing of personal data malfunction. The Party must further plan for how the restart or restoration is to be achieved after such a malfunction.

### Accuracy

* 1. Each Party shall ensure that personal data processed in information systems are correct in the sense that they are not subject to distortion and also correspond to its source, if applicable.

### Confidentiality

#### Pseudonymization

* 1. Personal data disclosed to a Party, or other recipient, shall be disclosed in pseudonymous form. A Party may not disclose code keys or other information that enables the identification of data subjects. Code keys or other information that enables the identification of data subjects may not be transferred to third countries without sufficient safeguards in place.
	2. In order to avoid misunderstanding: pseudonymized personal data provided to a Party, to a data processor or another recipient, or to a third party, is still considered personal data even if it is not possible for the recipient or the third party to identify the data subject who the personal data refers to. Pseudonymization is merely a security measure.

#### Evaluation of protection against unauthorized access

* 1. Each Party shall annually evaluate the protection against both internal and external unauthorized access to computer networks and IT-systems used for the processing of personal data.

#### Access control

* 1. Each Party shall be responsible for assigning each user an individual authorization for access to personal data (access control). A party shall develop routines for changing, removing, and regularly following up the authorizations to ensure that these are correct and current.

####  Authentication

* 1. Each Party shall be responsible for ensuring that each user can use his or her authorization only after it has been authenticated in a secure manner. This requires, as a minimum, that access can only take place with the help of strong authentication (two factors) unless the parties have agreed otherwise.

#### Physical protection

* 1. Each Party shall ensure that IT-systems used for the processing of personal data are physically protected against damage, interference, and unauthorized access.

#### Removable medium for information storage

* 1. Each Party that allows removable medium for the storage of personal data shall ensure that unauthorized persons cannot access that stored personal data, and that personal data on such medium is not lost.
	2. Information storage medium containing personal data shall be phased out in such a way that the data cannot be read or recreated.

### Traceability

* 1. Parties shall be responsible for:
		1. the documentation of the access (logs) securely indicates which access and other measures have been taken with personal data,
		2. the logs securely indicate at which business unit the measures were taken,
		3. the logs securely indicate at what time and date the measures were taken,
		4. the logs securely indicate the user identity of whom has taken the measures,
		5. systematic and periodic random checks, or other forms of inspection, of the logs are performed,
		6. these checks are documented, and,
		7. the logs are stored for at least five (5) years to enable control of access to personal data.

### Compliance

* 1. In order to check compliance with this Annex 4, the Party shall ensure that a self-inspection, or inspection by an independent third party, is carried out at least once a year. Such inspection must be documented. If a Party chooses to carry out a self-inspection, that Party shall ensure that the person or persons carrying out the self-inspection have expertise in information security and are independent in how the self-inspection is to be executed.

### Education

#### Awareness training regarding personal data breach

* 1. Each party shall annually ensure that employees under its direction receive appropriate training and education in how a personal data breach is identified and reported.

## Appendix 5 – Personal data processors

### [Processor A]

|  |  |
| --- | --- |
| The Party which intends to let a data processor process personal data on its behalf: |  |
| The company name and registered office of the data processor: |  |
| Types of personal data and categories of data subjects: |  |
| Whether personal data is to be transferred to a third country for processing: |  |