

General information security annex

I Purpose and application of this document

- #1 This document is an annex to the Agreement concluded between the Contracting Parties by which matters related to the data protection, information security and processing and secrecy of HUS's material of the subject of the Agreement are agreed upon. This annex shall be applied in accordance with the order of precedence of contract documents stated in the Agreement, with due regard to what is stated below on the application of potential limitations of liability under the Agreement. Terms pertaining to HUS's material shall be applied for as long as the Processor has any material of HUS in their possession, even after the Agreement period has ended. Any references to the Agreement in this annex means the Master Agreement and all its annexes, unless otherwise stated.

2 Definitions

- #2 *Personal data*: Defined in Article 4 of the Data Protection Regulation.
- #3 *Processing of personal data*: Defined in Article 4 of the Data Protection Regulation. Processing of personal data refers, for example, to the Processor's opportunity to view personal data in connection with the implementation of the subject of the Agreement.
- #4 *Confidential information*: Professional secrets concerning a Contracting Party and its operating units, contracting partners or other partners, information concerning security and emergency response arrangements, other information that is to be kept confidential under the Act on the Openness of Government Activities (621/1999) or otherwise considered confidential and secret, as well as personal data.
- #5 *Data Protection Regulation*: Regulation (EU) 2016/679 of the European Parliament and of the Council 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.
- #6 *HUS's material*: HUS's documents, written information, databases and software to be used in connection with the supply of the product or in connection with the service, and other material that HUS has submitted to the Processor for the purpose of providing a product or a service, including data material that is created when the service or product is used, its design, structure and metadata. The structure of the data material does not refer to its structure in terms of storage technology but to its conceptual design and parsing for the purposes of HUS. Storage technically, the data material can be contained in files, databases or other storage formats. In this definition, data content and data refer to both raw data and processed data.

3 Sub-processors

- #7 The obligations imposed in this Annex on the Processor and the individuals in the Processor's employ shall also apply to the Processor's sub-processors and the individuals in their employ insofar as they contribute to the implementation of the subject of the Agreement. The Processor shall inform sub-processors of these obligations and ensure that its sub-processors and all of the individuals in their employ abide by them. The Processor shall be responsible for the performance of the sub-processors used as for its own. The Processor shall ensure the right to perform audits laid out in the Agreement can be extended to the sub-processor.

4 General obligations

4.1 Contracting Parties' obligation to comply with legislation

- #8 The Contracting Parties undertake to comply with the legislation on information security, data protection, publicity and secrecy and the official regulations issued thereunder. The Agreement does not derogate from the mandatory obligations imposed on a Contracting Party by law.

4.2 Obligation to co-operate

- #9 The Contracting Parties will use all reasonable endeavours to contribute to the attainment of a high level of information security in the implementation of the subject of the Agreement and to the other Contracting Party's opportunity to maintain it on its own part.

4.3 Due care obligation

- #10 The Contracting Parties must ensure that the duties foreseen hereunder are carried out with due care and that the confidentiality, availability or integrity of HUS's material or confidential information is not endangered as a result of negligence, incorrect working methods or other conduct at variance with the Agreement by the employees of the Contracting Parties.

4.4 Duties and responsibilities pertaining to information security

- #11 The Contracting Parties shall define within their organisation the duties and responsibilities pertaining to information security, as well as appoint a sufficiently experienced and qualified person in charge.

4.5 In-house information security instructions

- #12 The Contracting Parties shall comply with their in-house information security instructions insofar as they are not in conflict with the Agreement and this Annex.

5 HUS's material

5.1 Handling

- #13 In the handling of HUS's material, the Processor shall comply with any reasonable guidelines given by HUS as well as for its part the data security measures required under the Act on Information Management in Public Administration (906/2019). If the Processor prepares or processes patient documents under the Agreement, the Processor commits to preparing and processing the said documents in accordance with the specific rules for preparing and processing patient documents and the instructions given by HUS. In addition, patient documents prepared by the Processor are, among others, part of HUS's material.

5.2 Intended use

- #14 The Processor may only use HUS's material for the implementation of the subject of the Agreement and only to the extent that is necessary for the implementation of the subject of the Agreement. The Processor shall see to it that HUS's material is only processed by individuals working for and on behalf of the Processor whose work duties involve the processing HUS's material.

5.3 Information requests

- #15 The Processor shall forward any third-party information requests concerning HUS's material immediately to HUS.

5.4 Returning HUS's material

- #16 Upon expiry of the Agreement or when the need to use the material no longer exists, the Processor shall return HUS's up-to-date material to HUS within 14 days of HUS's written request to this effect in accordance with the data material openness requirement. The data material openness requirement means that the data material of HUS is available in a generally used format and accessible with generally used information systems without any royalties or licence fees or other conditions limiting its use. The Processor is not entitled to any separate compensation for the delivery of HUS's material in accordance with this subparagraph 5.5.

5.5 Destroying HUS's material

- #17 The Processor shall, at its own cost, destroy any copies of HUS's material in a data secure manner when HUS has confirmed, in writing, that HUS's material had been returned in accordance with the Agreement. The Processor shall, at HUS's request, present reasonable evidence of destroying the material without any separate compensation. The Processor is not liable to destroy the material if the Processor is obligated to retain the material concerned under law or official regulation.

6 Processing of personal data

- #18 This paragraph 6 shall apply in the event that the Processor processes personal data under the Agreement. Also the conditions concerning HUS's material, among others, shall be applied to the processing of personal data.

6.1 Processor's right to process personal data

- #19 HUS or the sub-processor of HUS is a Controller within the meaning of data protection legislation and the Processor a Processor of personal data. If the data of HUS consists of data derived from various Controllers, remains the obligation to keep them separate, as demanded by the data protection legislation, with the Processor.
- #20 The Processor shall have the right to process the personal data contained in HUS's material
- only on the grounds indicated in the Agreement or with HUS's prior written permission;
 - only to the extent and as long as it is necessary for the implementation of the subject of the Agreement;
 - only in accordance with the data protection legislation, this Agreement and the documented instructions separately given by HUS.
- #21 The following matters are addressed in greater detail in the Agreement or the related documentation:
- the subject and duration of the processing of personal data;
 - the nature and purpose of the processing of personal data;
 - the type of the personal data;
 - the categories of data subjects;
 - the controller's obligations and rights (insofar as they have not been indicated in this Annex).
- #22 If a Contracting Party considers that the aforementioned matters or other requirements of data protection legislation are not indicated in the said documents in a sufficiently precise manner, the Contracting Party has the right to request that the matters concerned be recorded as part of the contract documents or documentation.

6.2 Familiarity with and adherence to data protection legislation

- #23 The Processor ensures it is familiar with the data protection legislation on the processing of personal data as it pertains to the Agreement, including the obligations set to the processor of personal data, as specified in the Articles 28 and 32 of the Data Protection Regulation. Any conduct of the Processor that is contrary to the data protection legislation may be considered a material breach of contract.
- #24 The Processor shall immediately notify HUS if it suspects that the Agreement or the instructions or any practice used in the implementation of the subject of the Agreement are at variance with data protection legislation.

6.3 Actions to secure compliance with the data protection legislation

- #25 The Processor is required to assess the risks associated with processing of personal data in view of the data subjects and to implement appropriate technical and organisational measures to ensure that the processing of personal data meets the requirements of data protection legislation and to safeguard the protection of the rights of the data subject. The technical and organisational measures must be recorded in writing and the documentation must be kept up-to-date. Among other things, the Processor shall see to the proper protection of the personal data it processes to ensure their confidentiality, integrity and availability, and abide by the principle of data protection by design and by default in the implementation of the subject of the Agreement.
- #26 The Processor shall designate a data protection officer pursuant to Article 37 of the Data Protection Regulation, or a person in charge of data protection and communicate their contact details on their public website or directly to HUS.

6.4 Use of other processors of personal data

- #27 The Processor may use sub-processors to process personal data. The Processor shall notify HUS in advance in writing of any planned changes concerning the adding or replacement of other processors of personal data, in which case HUS may, for a well-founded reason, deny such change. The Processor is responsible for ensuring that a proper contract that meets the obligations posed by data protection legislation has been concluded between the Processor and the other processor of personal data.

6.5 Processor's obligation to assist and provide information

- #28 The Processor shall assist HUS in fulfilling its obligation to respond to requests that concern the exercise of the data subject's rights pursuant to data protection legislation and in ensuring that the obligations set forth in Articles 32 through 36 of the Data Protection Regulation are complied with. Among other things, the Processor shall assist HUS in making the notifications and communications required under Articles 33 and 34 of the Data Protection Regulation to the supervisory authority and the data subject within the time period specified in the Data Protection Regulation. The Processor shall also, on request, cooperate with the supervisory authority as provided under Article 31 in the performance of its tasks.
- #29 The Processor shall provide HUS with all the information that is necessary for proving compliance with the obligations imposed by data protection legislation. The Processor shall constantly maintain the said information and assess the adequacy of the actions.
- #30 The Processor shall, on its own initiative, communicate to HUS the places where the processing of personal data takes place and any changes to them if they are not clearly stated in the Agreement or in the documentation available to HUS.
- #31 HUS is responsible for the preparation of the required privacy statement, record of processing activities, and impact assessment, and for the implementation of prior

consultation. The Processor will provide HUS with information for their preparation and implementation.

- #32 The Processor shall fulfil its obligation to assist and provide information under this subparagraph 6.5 without any separate compensation.

6.6 Processing of personal data abroad

- #33 Unless otherwise expressly stated in the Agreement, the Processor or its sub-processor may not process the personal data outside of the EEA.
- #34 If the Processor or its sub-processor is authorised in the Agreement to process personal data outside of the EEA, the Processor shall be responsible for ensuring that the transfer outside of the EEA takes place pursuant to data protection legislation.
- #35 If the Processor processes personal data, as authorised in the Agreement, in the United States or in non-EEA countries other than those listed as trusted countries by the European Commission, the Contracting Parties must conclude an Agreement with HUS prior to starting the processing of personal data, in accordance with standard clauses as approved by the European Commission (Controller to Processor). If the processing of personal data is performed by the Processor's sub-processor, the Processor must enter into an equivalent agreement with its sub-processor (Processor to Processor). At HUS's request, the Processor must present the latter agreement to HUS.
- #36 As an alternative to an agreement concluded in accordance with standard clauses, the Processor may present an account stating that the binding rules (Binding Corporate Rules) as laid out in Article 47 of the Data Protection Regulation apply to the Processor or the sub-processor, and that the rules have been confirmed by the supervisory authority and that they apply to the relevant processing at hand.
- #37 The Processor agrees to undertake to transfer the processing of personal data on its own expense to a country located within the EEA or to a trusted country as listed by the European Commission or by executing the contract arrangement as provided in section 6.6 without undue delay if the processing country is removed from the list of trusted countries at its own cost. Similarly, if a contract made using the standard clauses or the aforementioned binding rule are later not considered to adequately fulfil the obligations laid out in data protection legislation, the Processor and HUS in collaboration shall be required to make the processing of personal data compliant with said legislation without delay.

6.7 Damages

- #38 If a Contracting Party has had to pay restitution for violations against data protection legislation, this Contracting Party is entitled to seek compensation from the other Contracting Party that has taken part in the same data handling for the other Contracting Party's share of the violations that have incurred. The liability of each Contracting Party is determined by Article 82 of the Data Protection Regulation. Any terms concerning limitation of liability in the Master Agreement shall not apply to the payment of compensation stipulated in this section.

7 Processors obligations to notify and report

7.1 Obligation to notify

- #39 The Processor shall, without undue delay, notify HUS of any circumstances that have come to the Processor's attention that may have an effect on the information security related to the subject of the Agreement and of the measures and any consequences resulting from them. The obligation concerns, among other things, information security risks, changes to security arrangements, actual or attempted information security violations, unpatched system vulnerabilities, denial-of-service attacks and other similar nonconformances that are likely increase the risk posed to the confidentiality, integrity and availability of HUS's material. The Processor shall inform HUS of a responsible person to provide further information.
- #40 If the aforementioned report has to do with personal data breach, the report must be made without undue delay. The Processor shall take into account HUS's obligation pursuant to Article 33 of the Data Protection Regulation to notify on personal data breach to the supervisory authority within 72 hours e.g. by sending a preliminary report as soon as they find out about the matter, and supplementing it as new information becomes available. The report must, at the minimum,
- describe the nature of personal data breach with its likely consequences;
 - report on the categories of data subjects concerned and their estimated quantities, as well as the categories of personal information and their estimated quantities as accurately as possible;
 - describe the actions that have been taken or the actions that the Processor considers necessary due to the personal data breach or mitigating its possible consequences.
- #41 The Processor shall notify HUS of any changes to the documentation related to information security and provide HUS with up-to-date documentation without delay.

7.2 Periodic reporting

- #42 The Processor shall monitor the attainment of the level of information security specified in the Agreement on a regular basis and in a systematic manner. The Processor shall record any nonconformances and report them to HUS without delay and initiate corrective actions as soon as possible.

8 Action in the event of an information security breach

- #43 The Processor shall have in place written instructions on how to act in the event of information security breaches.
- #44 The Processor shall take care of the management of disruptions in accordance with the Agreement in such a way that problem limitation and repair is carried out immediately in compliance with the jointly agreed upon procedures.

- #45 The Processor shall be liable to assist HUS in minimising the damage related to data security breaches and in clarifying the matter with the authorities.
- #46 The Processor may charge the price specified in the Agreement for the additional work resulting from the information security breach if all of the following preconditions are met:
- the information security breach does not result from a cause the Processor is responsible for;
 - the Processor's error or omission has not contributed to the occurrence of the information security breach;
 - the actions taken by the Processor are not included in the potential charge for continuous service.

9 Processor's personnel

9.1 Non-disclosure obligation of the personnel

- #47 The Processor is responsible for ensuring that the individuals working for and on behalf of the Processor who may have access to HUS's confidential information, HUS's information systems or independently to HUS's facilities, have signed a written non-disclosure agreement beforehand and that they have sufficient information security expertise, considering their tasks. The Processor shall produce a reasonable account of the contents and signing of such non-disclosure agreement and of the information security expertise of their individuals, such as the training they have received, to HUS on request. HUS can also require that the individuals in question complete an information security online training provided by HUS.
- #48 The Processor shall see to it that the individuals working for and on behalf of the Processor are aware of the following provisions and undertake to abide by them:
- An employee may only use HUS's material for the purposes of their work duties and only insofar as this is necessary for the discharge of their work duties. An employee is not entitled to use HUS's material for any purposes other than said purpose.
 - An employee shall hold HUS's material in confidence and may not surrender or otherwise disclose it to third parties. The non-disclosure obligation shall survive the expiry of the Agreement. The non-disclosure obligation does not pertain to material that is part of the public domain.
 - Third parties shall include any individuals working for and on behalf of the Processor who, based on their work duties, do not need access to HUS's material.
 - An employee is required to immediately notify HUS or the Processor of any circumstances they become aware of that may endanger information security or data protection.
 - The Processor shall process the documents and records that contain HUS's material with care, ensuring sufficient information security. Any documents or records that contain HUS's material may not be taken outside HUS's or the Processor's facilities unless the employee's work duties specifically so require.

- The employee shall return any documents and records in their possession in a reliable manner while ensuring sufficient information security when the need to use the material for the discharge of their work duties no longer exists.
- The use of information systems creates log data that shall be monitored, as necessary.
- The breach of the non-disclosure obligation may incur personal liability on the employee as prescribed by the applicable legislation.

#49 The Processor shall also see to it that the individuals working for and on behalf of the Processor are aware of any other non-disclosure obligations under the Agreement and monitor the compliance of their actions with the Agreement.

9.2 Security clearance

#50 HUS shall have the right to require that security clearance in accordance with the Security Clearance Act (726/2014) or a foreign security clearance of equivalent level be requested in respect of the individuals working for and on behalf of the Processor who may have access to HUS's confidential information. The Processor shall be responsible for obtaining consent from the individual who is the subject of the clearance and for ensuring that the individual concerned provides the information necessary for carrying out the security clearance. If the individual who is the subject of the clearance refuses the clearance, the Processor shall appoint another individual with similar experience and competence for replacement.

#51 Each Contracting Party shall be responsible for the costs incurred by it from requesting the security clearance. HUS shall pay the regulatory charges related to requesting the security clearance.

10 Facilities and the use of information systems

10.1 Processor's in-house information security

#52 The Processor shall ensure the information security of its information systems, equipment and data communications systems it uses for delivering the subject of the Agreement. The Processor shall only use such information systems, equipment and data communications systems for delivering the subject of the Agreement whose information security risks the Processor is capable of monitoring and controlling and whose information security can be audited. If a piece of equipment used for implementing the subject of the Agreement is connected to information network, it shall be provided with up-to-date malware protection.

10.2 Processor's facilities

#53 The Processor shall be responsible for ensuring that the Processor's facilities where HUS's confidential information is processed or stored meet the following requirements:

- The facilities are properly protected with locking and other necessary measures to prevent unauthorised access.
- The proper physical protection of the facilities has been ensured in view of fire, power outages, water damage, outside interference and other similar special circumstances.
- Individuals whose work duties do not involve the processing of confidential information are not present in the facilities without supervision, unless the confidential information is stored in such a way that these individuals cannot access it.

10.3 Supervision of access rights

- #54 The Processor shall implement the subject of the Agreement in such a way that user rights to HUS's systems and HUS's material and to the related log, administration and configuration data will only be granted to individuals who need such rights in the discharge of their work duties. The Processor shall maintain an up-to-date list of access rights and the grounds for them.
- #55 The Processor shall maintain an up-to-date list of the individuals' access rights to the facilities where they have the opportunity to access HUS's material, systems or equipment.
- #56 The Processor shall remove any unnecessary access rights without delay e.g. in the event that an individual resigns from the employ of the Processor or a sub-processor or the work duties of the individual concerned change. In addition, the Processor shall check the active user rights at least once a year.

10.4 Access to HUS's facilities

- #57 The individuals in the employ of the Processor may have access to HUS's facilities if this is necessary for the implementation of the subject of the Agreement. In this case, the individuals in the employ of the Processor are required to comply with the instructions given by the person in charge designated by HUS along with any general instructions that are to be complied with while in the premises, and wear a photo ID card.

10.5 Use of HUS's information systems

- #58 If an individual working for and on behalf of the Processor needs user credentials to HUS's information systems, they shall be granted in accordance with HUS's user authorisation management procedure. The user credential application is to be filled and delivered to HUS by the individual's superior or the Processor's person responsible for the production. If the individual may have access to confidential personal data, the user credentials application form must include the individual's Finnish social security number. If the individual does not have a Finnish social security number, a similar foreign identifying number or similar means of personal identification that HUS considers sufficient shall be included. If the individual who is the subject of the clearance refuses the clearance, the Processor shall appoint another individual with similar experience and competence for replacement.

- #59 The Processor shall see to it that the individuals working for and on behalf of the Processor who have been given user credentials are aware of the following provisions and undertake to abide by them:
- HUS's information systems may only be used for purposes consistent with the employee's work duties, to the extent agreed upon in the Agreement and in compliance with the instructions related to the use of HUS's information systems.
 - The following actions, in particular, are prohibited unless they have been separately agreed upon in the Agreement:
 - o viewing and processing of patient information included in the information systems and other confidential information for purposes other than the discharge of work duties;
 - o actions aiming at increasing user or administration rights to the systems;
 - o using the data communications connections of the systems as a gateway for passage to other parts of HUS's data communications network or outside it;
 - o utilising the systems or data communications for the purpose of determining the structure or details of, or the information contained in, HUS's data communications traffic or services;
 - o installing of software.
 - The employees shall take care of the personal user credentials, passwords and other authentication tools provided by HUS in such a way that they do not end up in the hands of, or become known by, others.
 - HUS shall have the right to limit the employee's user rights or cancel them altogether when deemed necessary.
- #60 The Processor must without delay inform HUS whenever a person working on the behalf of the Processor no longer require credentials for the HUS data system, for instance due to modified or concluded duties.

II Secrecy

- #61 The Contracting Parties must hold secret all confidential information that they receive from each other and undertake not to use the information for any purposes other than those set out in the Agreement and to only use the information to the extent necessary for purposes hereof. The Contracting Parties are responsible for ensuring that all individuals and sub-processors working for them and on behalf of them comply with this provision. This provision will survive the termination of the Agreement.
- #62 The confidentiality obligation does not apply to information which is generally available or public or which a Contracting Party has lawfully obtained from a source other than the other Contracting Party.
- #63 Upon expiry of the Agreement or the when the need to use the material no longer exists, a Contracting Party must return or, with the consent of the other Contracting

Party, destroy in a data secure manner, all confidential material of the other Contracting Party. No material may be destroyed if the law or an official regulation requires that it be retained.

- #64 A Contracting Party shall have the right to make use of the professional competence and experience acquired in connection with the delivery.
- #65 The Processor shall not have the right to use the Agreement as reference without HUS's written permission.
- #66 HUS is obligated to comply with its obligation under the Act on the Openness of Government Activities (621/1999), regardless of any contractual terms on confidentiality.

12 Other terms and conditions

12.1 Audits

- #67 The Processor must allow and participate in audits regarding information security and data protection carried out by HUS or an independent third party authorised by HUS.
- #68 The third party acting as the auditor cannot be the Processor's competitor with regard to the operations being audited. The Processor can require that the third party conclude a non-disclosure agreement equivalent to the non-disclosure obligation included in this Agreement.
- #69 HUS must notify the Processor in writing at least two weeks in advance of its intention to carry out or commission an audit. Audits can be carried out at maximum twice a year.
- #70 Unless otherwise agreed elsewhere in the Agreement, HUS shall bear the costs of the third party acting as the auditor and, in other respects, the Contracting Parties shall participate in the audits at their own expense.
- #71 This subparagraph 12.1 shall be without prejudice to other rights of inspection HUS may have pursuant to the Agreement.

12.2 Amendments to this annex due to reasons related to information security or data protection and additional work

- #72 In the event of changes to the information security or data protection legislation or official orders or recommendations on their interpretation, the Contracting Parties shall make the necessary amendments to this annex pursuant to the agreed-upon terms of changes to the Agreement.
- #73 HUS reserves the right to request that the Processor perform the necessary amount of additional work, if amendments to the Agreement or other HUS guidelines on the processing of personal data require it, at the Agreement price. The Processor shall bear the cost of any changes necessary due to changes in legislation or official orders that pertain directly to the Processor.