

ADDENDUM TO SUPPLIER AGREEMENT CONCERNING DATA PROTECTION

Between the undersigned

de VZW Onze-Lieve-Vrouw van Troost, exploitant van het A.Z. Sint-Blasius with registered office established at 9200 Dendermonde, Kroonveldlaan 50, BTW nr. BE0411.975.133, lawfully represented by [Name], CEO.

Hereinafter referred to as “**the Hospital**”

AND

.....
.....
.....[information completed by the supplier]

Hereinafter referred to as “**Supplier**”

Hereinafter collectively referred to as the “**Parties**”

Considering that

The Supplier provides services for the Hospital, as described in the Basic Agreement, these services entail the processing of personal data and the parties, through this Addendum, wish to establish the arrangements for the processing of personal data in the context of the services

the following has been agreed:

If the Parties wish, by mutual agreement, to make adjustments to the text of this Addendum, such adjustments – in so far as they comply with the Data Protection Legislation and fall within the scope of the contractual freedom of the Parties – shall be recorded, stating the reason, in Annex 1 to this Addendum.

Changes to Annex 1 shall be valid only if they have been signed and dated by both parties.

1. DEFINITIONS

1.1 For the application of this Addendum, the following definitions shall apply:

- **General Data Protection Regulation:** 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, with its amendments and European implementing legislation;
- **Data Protection Legislation:** the General Data Protection Regulation, other European legislation containing provisions concerning data protection and privacy, as well as the applicable national legislation on data protection and privacy in the Member States, with its amendments and implementing decrees, including the approved codes of conduct applicable to the sector.
- **Personal data, Processing, Controller, Processor, Data Subject, Consent:** the definitions as set out in the General Data Protection Regulation;
- **Basic Agreement:** the agreement between the Hospital and the Supplier: **[date]** regarding tot **[fill in the title of the agreement and any reference number]**.

1.2 The Supplier shall provide services to the Hospital on the basis of, and as defined in, the Basic Agreement.

For the processing activities as specified in **Annex 2** to this Addendum, the following qualification shall apply:

- the Hospital shall determine the purpose and means of processing and shall consequently be the controller;
- the Supplier shall carry out the processing of personal data on behalf of the Hospital as controller, and shall consequently be the processor.

2. SCOPE AND RELATIONSHIP TO THE BASIC AGREEMENT

- 2.1** This Addendum shall form an integral part of the Basic Agreement concluded between the Hospital and the Supplier. The provisions of this Addendum shall apply in full to all processing of personal data performed by the Supplier in the context of the implementation of the processing activities specified in Annex 2.
- 2.2** The provisions of this Addendum (and Annexes) shall take priority over the (possibly contrary) provisions concerning data protection and processing and confidentiality of data in the Basic Agreement, and shall replace these provisions.

3. PROCESSING IN ACCORDANCE WITH THE REGULATIONS AND THE WRITTEN INSTRUCTIONS OF THE HOSPITAL

- 3.1** When processing personal data, the Parties shall act in accordance with the Data Protection Legislation.
- 3.2** The Supplier shall process the personal data exclusively on the basis of the written instructions of the Hospital, unilaterally determined by the Hospital and as set out in **Annex 2** to this Addendum. If the written instructions are not clear, the Supplier shall notify the Hospital of this in writing, whereupon the instructions shall be clarified by common accord.
- 3.3** Unless otherwise stipulated in this Addendum, the Supplier shall not process the personal data for its own purposes or for those of third parties, or provide the personal data to third parties, or transmit these data to a country located outside the European Union without having received a written instruction to do so from the Hospital. Processing in accordance with the instructions of the Hospital may also mean that the processing must be stopped (immediately).

If European or national legislation requires the Supplier to undertake specific processing, the Supplier shall inform the Hospital, prior to the processing, of that legal requirement, unless this legislation prohibits such notification for important grounds of general interest.

- 3.4** The Hospital shall give instructions to the Supplier in accordance with the Data Protection Legislation and shall ensure that all personal data entrusted to the Supplier have been obtained lawfully and can be processed under the Basic Agreement.

4. APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES

- 4.1** The Parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in accordance with Article 32 of the GDPR.
- 4.2** When determining the measures, the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of persons, shall be taken into account.

The measures shall include, inter alia, as appropriate:

- Pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

- 4.3** In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

The Supplier shall adhere to the standards of approved codes of conduct and certification mechanisms as applicable within the sector. He attaches proof thereof as an Annex to this Addendum.

- 4.4** The Supplier shall describe in **Annex 3** the appropriate technical and organizational measures that it shall take. It shall report on its own initiative to the Hospital the changes that are implemented to the measures as set out in Annex 3, and this within a period of fourteen days after the changes have been made.

5. PROCESSING BY A “SUB-PROCESSOR” OR EMPLOYEE

- 5.1** The Supplier shall ensure that its representatives, agents, subcontractors and employees comply with the provisions of this Addendum. The Supplier shall only share or make available personal data of the Hospital to the representatives, agents, subcontractors and employees directly involved in the performance of the Basic Agreement on a need-to-know basis.

The Supplier shall ensure, in line with this:

- that persons authorised to process personal data have undertaken to maintain confidentiality or are bound by an appropriate statutory obligation of confidentiality;
- that measures have been implemented to ensure that any natural person acting under its authority who has access to the personal data, shall not process these data except on instructions from the Hospital, unless required to process them by European or national legislation.

- 5.2** The Supplier is only permitted to engage a third party as a sub-processor if it has informed the Hospital in a timely manner and in any event in advance of the identity of the sub-processor and if the Hospital has not objected to this. If the Hospital raises any objection (on reasonable grounds) regarding the proposed new Sub-processor within 14 days of receipt of the Supplier's notification, the Supplier will not pass on any personal data of the Hospital to the proposed Sub-processor, unless with the prior written and explicit consent of the Hospital.

- 5.3** The Supplier shall provide the Hospital in Annex 2 with full details of the processing taken over by the subprocessor(s) to this Addendum.

- 5.4** If during the term of the agreement the Supplier uses other sub-processors than the sub-processors initially mentioned in Annex 2 or if there are any changes regarding the data in Annex 2, the Supplier will inform the Hospital thereof without delay. If the Hospital raises any objection (on reasonable grounds) regarding the proposed new Sub-processor within 14 days of receipt of the notification from the Supplier, the Supplier will not transfer any personal data of the Hospital to the proposed Sub-processor, except with the prior written and explicit consent of the Hospital. Annex 2 will be amended in such case.

- 5.5** When the Supplier uses a subprocessor, the Supplier shall impose on this subprocessor by agreement the same data protection obligations as those applicable between the Processor and the Controller. The Supplier shall provide the Hospital with the agreement with the subprocessor upon first request.
- 5.6** If the sub-processor fails to comply with its data protection obligations, the Supplier shall remain fully liable in relation to the Hospital for complying with the sub-processor's obligations.

6. PERSONAL DATA TRANSFERS OUTSIDE THE EEA

- 6.1** If personal data is transferred to a country or organization outside the European Economic Area, the Supplier will comply with the guarantees of Chapter 5 GDPR and provide appropriate safeguards. The Supplier will inform the Hospital of any transfer outside the European Economic Area:
- The country of transfer
 - The transfer instrument
 - The analysis and assessment of the additional measures to be taken to implement the transfer (Transfer Impact Assessment (TIA)).
- 6.2** If the Supplier will process the personal data outside the European Economic Area, the Hospital may request the aforementioned analysis and assessment of the law and/or applicable practices of the third country and the additional measures from the Supplier. The Supplier will provide this assessment (Transfer Impact Assessment) at the first request of the hospital.
- 6.3** If the specific transfer instrument of art. 45 to 49 GDPR is not effective and no additional measures are taken to safeguard the level of data protection as laid down in the GDPR, the Supplier is not permitted to transfer the personal data outside the European Economic Area, unless the Hospital has given its prior written consent to do so.
- 6.4** This article also applies to any transfers made by the Subprocessors that the Supplier uses for the processing of personal data on behalf of the Hospital.

7. PROVISION OF ASSISTANCE WITH RESPECT TO THE OBLIGATIONS REGARDING THE DATA PROTECTION POLICY OF THE HOSPITAL

7.1 Taking into account the nature of the processing and the information available to it, the Supplier shall undertake to provide assistance to the Hospital with respect to the responsibility of the Hospital to comply with the following data protection obligations:

- Implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk;
- Notification of a personal data breach to the supervisory authority;
- Communication of a personal data breach to the data subject;
- Carrying out a data protection impact assessment;
- Consultation of the supervisory authority prior to processing where the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Hospital to mitigate the risk.

The time and resources spent by the Supplier in providing the assistance shall be at the Supplier's own expense.

7.2 Pursuant to Article **Fout! Verwijzingsbron niet gevonden.**, the Supplier shall inform the Hospital in detail and immediately of a (suspected) personal data breach as well as of any data leak (at the sub-processor too) as soon as the Supplier has become aware of this. The notification shall take place in such a way that the Hospital can satisfy in time its legal obligations as controller under the Data Protection Legislation. The Supplier shall indemnify the Hospital in accordance with Article **Fout! Verwijzingsbron niet gevonden.**

The Supplier shall use the report form in **Annex 4** for the reporting.

The Supplier shall also provide assistance in the investigation and the mitigation and remediation of a personal data breach. In this respect, it shall provide assistance, inter alia, with a view to the documentation of measures such as data protection by design and data protection by default.

7.3 The Supplier shall notify the Hospital immediately of any complaint, accusation or request made (including if it comes from a regulator) with regard to the processing of personal data by the Supplier. The Supplier shall offer all necessary cooperation and support that the Hospital can reasonably expect with regard to such a complaint, accusation or request, including by providing full information on such a complaint, accusation or request, together with a copy of the personal data concerning the data subject in the possession of the Supplier.

8. PROVISION OF ASSISTANCE FOR REQUESTS BY THE DATA SUBJECTS

- 8.1** Taking into account the nature of the processing, the Supplier shall provide the Hospital with assistance by appropriate technical and organisational measures in fulfilling the Hospital's obligation to respond to requests to exercise the rights of the data subject, as specified in the Data Protection Legislation.

This implies, inter alia:

- that the Supplier provides all the personal data requested by the Hospital within the (reasonable) period of time requested by the Hospital, in any case including the full details and copies of the complaint, communication or request and any personal data in its possession concerning the data subject;
- that the Supplier implements technical and organisational measures that permit the Hospital to reply effectively and in a timely manner to relevant complaints, communications or requests.

The time and resources spent by the Supplier in providing the assistance shall be at the Supplier's own expense.

- 8.2** Pursuant to Article **Fout! Verwijzingsbron niet gevonden.**, the Supplier shall undertake to inform the Hospital without delay if it receives one of the following requests from a data subject (or third party acting on behalf of a data subject):

- a request for access to the data subject's personal data processed;
- a request for rectification of incorrect personal data;
- a request for erasure of personal data;
- a request for restriction of the processing of personal data;
- a request to obtain a portable copy of the personal data, or for transmission of a copy to a third party;
- an objection to any processing of personal data; or
- any other request, complaint or communication concerning the obligations of the Hospital under the Data Protection Legislation.

The Supplier shall not reply to the requests and applications by the data subject itself, unless there are any written agreements to the contrary between the Hospital and the Supplier.

9. RIGHT OF CONTROL BY THE HOSPITAL

- 9.1** The Hospital shall have the right at any time to check compliance by the Supplier with the Addendum.

The Supplier shall make all information available to the Hospital which is needed to demonstrate compliance with the obligations under the Data Protection Legislation.

The Supplier shall make audits possible, including inspections, by the Hospital or an auditor authorised by the Hospital, and shall contribute to them. These audits can be announced, but also unannounced in the event of suspected irregularities. The Supplier shall grant full cooperation with regard to such an audit and, at the request of the Hospital, shall supply evidence of compliance with its obligations under this Addendum.

- 9.2** The Supplier shall inform the Hospital immediately if, in its opinion, an instruction under Article 9.1 breaches the Data Protection Legislation.

10. LIABILITY

- 10.1** The Parties shall each be responsible and liable for their own actions. The liability regulated in this Article shall relate exclusively to the liability arising from a breach of the Data Protection Legislation and this Addendum.
- 10.2** The Supplier shall reimburse and indemnify the Hospital for all claims, actions, demands by third parties and for all damage and losses (also including fines imposed by the data protection authority) arising directly or indirectly from processing of personal data if, during the processing, it has not complied with the obligations of the Data Protection Legislation addressed specifically to processors or if it has acted outside or contrary to the lawful instructions of the Hospital.
- 10.3** The Parties shall ensure sufficient cover of their liability.

11. END OF THE AGREEMENT

- 11.1** If the Supplier fails to comply correctly with the obligations arising from this Addendum or fails to implement appropriate measures within a maximum period of two months, the Hospital – without prejudice to other forms of termination as provided for in the Basic Agreement – may terminate the Basic Agreement immediately after the aforementioned period of two months and/or stop the processing assignment.
- 11.2** This agreement shall form an integral part of the Basic Agreement and shall therefore follow the fate of the Basic Agreement. However, if the Basic Agreement comes to an end, the provisions of this Addendum shall apply as far as necessary for winding up the obligations in accordance with the Data Protection Legislation.
- 11.3** Immediately on (no matter which) termination or expiry of the Basic Agreement or after the expiry of the storage period, the Supplier – at the discretion of the Hospital – shall return the personal data to the Hospital and/or irrevocably erase the personal data entirely and remove existing copies. If the Hospital opts for the removal of the personal data, the Supplier shall demonstrate to the Hospital, on written request, that the removal has in fact occurred.

The Supplier may derogate from paragraph 1 if the storage of the personal data is required under European or national legislation.

12. FINAL PROVISIONS

- 12.1** In the event of nullity or voidability of one or more provisions of this Addendum, the other provisions shall remain in full force.
- 12.2** This Addendum shall be subject to Belgian law. Disputes shall be brought before the courts/tribunals in the judicial district of Oost-Vlaanderen, division Dendermonde, which shall have exclusive territorial jurisdiction.

The contract should be drawn up in duplicate, one for each party at
on..... .

[Name]

The Hospital

[Name]

Supplier

Annexes

- Annex 1: Adjustments to the addendum under contractual freedom of the parties
- Annex 2: The processing assignment and instructions, as specified by the hospital
- Annex 3: The information security questionnaire
- Annex 4: Model form for reporting of data leaks
- Annex 5: Questionnaire in case of use of cloud services

ANNEX 1 – ADJUSTMENTS TO THE ADDENDUM UNDER CONTRACTUAL FREEDOM OF THE PARTIES

The Addendum contains a standard text which implements the obligations arising from the Data Protection Legislation. Certain aspects fall (within certain limits) under the contractual freedom of the parties.

If the Parties wish to regulate certain aspects differently or more specifically or wish to add certain matters, these are determined explicitly in this Annex.

Contractual freedom can cover, for example:

- the periods within which the Supplier must inform the Hospital or must provide assistance (but in each case within the period within which the Hospital must itself report to the supervisory authority or the department concerned);
- specification of whether specific or general consent is applied for the sub-processor(s);
- ...

Changes in this Annex are valid and enforceable only if this Annex has been signed and dated by both parties.

Article	Text which lapses or may lapse	Replacement or additional text	Reason

Thus agreed and drawn up in duplicate at on

[Name]

The Hospital

[Name]

Supplier

ANNEX 2 - THE PROCESSING ASSIGNMENT AND INSTRUCTIONS AS SPECIFIED BY THE HOSPITAL

Accompanying note

This Annex describes the specific processing by the Supplier, for which the Hospital gives instructions at the time of the conclusion of the Basic Agreement or on signing the Addendum.

Changes and/or supplements to this Annex 2 occur in each case via a separate document which is added as an Appendix to this Annex 2 (Appendix 1 to Annex 2; Appendix 2 to Annex 2, etc.), which is dated and which shows the explicit and written instruction and/or agreement of the Hospital.

I. The purpose of the processing of personal data

The processing of Personal Data by the Supplier takes place under the implementation of the Basic Agreement concerning..... **[to be completed by supplier].**

Description of the services under the Basic Agreement and nature and purpose of the processing of personal data in the context of the services:

.....

II. The categories of personal data which the Hospital instructs the Supplier to process (indicate what is applicable and if necessary supplement):

- contact details
- financial data
- invoice data
- wage data
- medical data
- marketing data
- data on the use by the Hospital of the services and related products of the Supplier
- other (to be specified):

.....

III. The categories of data subjects whose personal data are processed (indicate what is applicable and if necessary supplement):

- Hospital patients

- trusted persons, representatives and contact persons of the Hospital patients
- carers of the Hospital patients
- Hospital staff members
- other (to be specified):

.....

.....

.....

.....

IV. The processing of the personal data (indicate what is applicable and adapt/supplement where necessary):

The Hospital hereby gives the following instructions for the processing of personal data (without prejudice to the instructions arising directly from the provisions of the Basic Agreement or this Addendum or which are reasonably required for the Supplier to fulfil its obligations correctly):

- Consultation of personal data
This refers to services provided by the Supplier whereby personal data of the Hospital can be viewed by staff or Subcontractors of the Supplier, including, but not limited to, servicedesk Services, (remote) monitoring Services, system management Services, technical application management, vulnerability scanning Services, reporting Services in governance and software asset management Services.
- Storage of personal data
This refers to services provided by the Supplier whereby personal data of the Hospital are stored in a storage system delivered by the Supplier, such as, but not limited to, cloud storage Services, cloud back-up Services, file Services, directory Services, managed file transfer, mail & calendaring and logfile processing.
- Transmission of personal data
This refers to services provided by the Supplier whereby personal data of the Hospital are transmitted by, to or between applications on a platform managed by the Supplier, including, but not limited to, LAN Services, Wide Area Network Services, data centre interconnectivity Services, Loadbalancing, SAN switch interconnects and Services provided using the Voice over Internet Protocol (VoIP).
- Adaptation or alteration of personal data
This refers to services provided by the Supplier whereby personal data of the Hospital can be adapted either manually or automatically, such as in an automated job flow supported by a job scheduling system.
- Software tests
This refers to services provided by the Supplier in which databases of the Hospital containing personal data (personal data which have not been anonymised) are used outside the production environment (in test, acceptance, etc.) as part of the testing process of the Hospital software application.

○ XXX

- XXX
- XXX
- XXX
- [To be completed]

IV. The storage periods of the (various categories of) personal data:

The Supplier stores the processed personal data in an appropriately secure manner for the period necessary to perform the written instructions of the Hospital, and with regard to the categories of personal data below, for the period specified below [complete if storage period can be expressed in months]:

- for [complete category of data] for [XX months after/from.... e.g. the last use]
- for [complete category of data] for [XX months after/from.... e.g. the last use]

V. The Data Protection Officer or other responsible contact persons for data protection and processing (complete):

For the Hospital

Name: Quinten Blindeman
Contact details: privacy@azsintblasius.be

For the Supplier

Name:
Contact details:

VI. List of the subprocessors

The processor will, depending on the agreed master agreement(s), use some or all of the following sub-processors and locations for its services

Please complete the list with all sub-processors, including apps, SaaS platforms, online accounts, cloud providers, software plug-ins, cookie based exchanges, etc.

<u>Name subprocessor</u>	<u>address of registered office</u>	<u>place of processing</u>	<u>nature of processing</u> <u>(description of the nature of processing, assets, ...)</u>

VII. List of transfers to third countries

<u>Data exporter</u>	<u>Data importer</u>	<u>country where the personal data is processed</u>	<u>transfer instrument (SCC, BCR, ...) and additional measures (if necessary) (*)</u>

(*) if the Hospital is a data exporter and the European Standard Contractual Clauses (ESCCs) of the European Commission are invoked, these ESCCs will be added as Annex 5 to the processing agreement

ANNEX 3 – INFORMATION SECURITY - QUESTIONNAIRE

QUESTIONNAIRE REGARDING THE PRESENCE AND EFFECTIVENESS OF ORGANISATIONAL AND TECHNICAL MEASURES FOR THE PROTECTION OF (PERSONAL) DATA

To be completed by the principal processor/principal contractor:

Answer each question and state the name and which supporting document you have available.

The answers to the questions must also relate to the processing by subprocessor(s).

QUESTIONS	NO	YES	REVIEWED	SUPPORTING_DOCUMENTS	short explanation
Description of the service					
Is the documentation regarding the service provided current and accurate?					
Organisational Measures					
ISO 5.1 - Is there a clear security policy covering all domains of ISO 27001/27002 – taking into account the described “dimensions to be considered”?					
ISO 5.2 - Are roles and responsibilities defined, particularly with regard to CISO, DPO, operational management, incident management?					
ISO 5.3 - Has segregation of duties been applied to make unauthorized actions impossible?					
ISO 5.12/5.13 - Is a classification of data and systems applied?					
ISO 5.16/5.17/5.18 - Is there strict user and access control? Especially for privileged administrators?					

ISO 5.19 - Are the contractual obligations passed on 1-on-1 to your sub-processors and do you monitor this at least annually?					
ISO 5.20 - Are all significant activities (particularly of administrators) recorded in immutable audit trails accessible to the controller?					
ISO 5.21/5.22/5.23 - Do you have clear rules regarding the delivery and use of software and hardware and (security) testing – applicable to every change?					
ISO 5.24 – Are there clear systems and processes for managing (and coordinating) security incidents?					
ISO 5.34 – Are you aware of and do you apply the rules regarding privacy protection and the protection of personal data?					
Personnel Measures					
ISO 6.1 / 6.2 / 6.3 – Are there clear rules and supervision of the behavior of privileged administrators? And are safety rules repeated annually in their training?					
ISO 6.4/6.5/6.6 - Are there clear rules in case of non-compliant behavior? When changing function or leaving the company? Are all your employees bound by a confidentiality clause?					
ISO 6.7 / 6.8 – Are there clear rules regarding remote working (only through processor systems) + reporting of any/possible security incidents?					

Physical Measures					
ISO 7.1/7.2/7.3/7.4 - Are the access to the systems and the systems used in management up to standard?					
ISO 7.5/7.6/7.7/7.8/7.10/7.11 - Have adequate measures been taken to make unauthorized access to systems and data carriers in principle impossible?					
Technological Measures					
ISO 8.1 – Do administrators have adequate and secure systems?					
ISO 8.2 / ISO 8.3 / ISO 8.4 - Do you have a separate privileged access management environment (PAM)? Is a VPN used for remote (management) access? And is access limited to a need-to-know?					
ISO 8.5 - Do you apply strong authentication to all your processes and MFA for all privileged access?					
ISO 8.7 / 8.8 – Are your systems maximally protected against malware? Do you adequately test your systems against vulnerabilities?					
ISO 8.10 / 8.11 / 8.12 / 8.13 – Are you protecting data adequately and in accordance with their CIA classification levels?					
ISO 8.14 – Do you have the necessary backup and disaster recovery systems in place according to the CIA classification?					
ISO 8.15/8.16 - Do you have adequate logging and monitoring to detect security incidents?					

ISO 8.20 / 8.21 / 8.22 – Is your infrastructure set up according to the rules of the art to adequately separate data and systems?					
ISO 8.24 – Do you apply adequate cryptographic measures such as signing or encryption where necessary?					
ISO 8.25 / 8.26 / 8.27 / 8.28 / 8.29 – Do you have a software delivery pipeline that validates every code/config change for errors/non-compliances...?					

If the processor uses public cloud services, he is also expected to complete the Annex 5 questionnaire

The processor,	
Name and position of the person signing on behalf of the processor (<i>legal representative – NOT the DPO</i>)	
Date	
I declare that the answers are correct and do not conceal any significant shortcomings. I undertake to provide the supporting documents in the event of an audit.	Signature

When did the breach take place?

- a. On (date + time)
- b. Between (date + time) and (date + time)
- c. Not yet established
- d. An anonymous report has been made by a third party

Establish context of the data involved in the breach:
Classification of the data:

- a. None, the data cannot be attributed to an individual
- b. Name and address data
- c. Telephone numbers
- d. E-mail addresses, Facebook IDs, Twitter IDs, etc.
- e. User names, passwords or other login data, customer numbers
- f. Financial data: account numbers, credit card numbers
- g. National registration number
- h. Copies of identity documents
- i. Gender, data of birth, and/or age
- j. Data concerning someone's religion or philosophy of life, race, political persuasion or membership of a trade union
- k. Data concerning someone's health or sexual orientation
- l. Personal data under criminal law or personal data about unlawful or annoying behaviour in connection with a prohibition imposed as a result of that behaviour
- m. Data about someone's financial or economic situation, data on debts, salary and payment data
- n. Derived financial data (income category, home ownership, car ownership)
- o. Lifestyle characteristics (including family composition, housing situation, interests, demographic characteristics (age, gender, nationality, profession, education)
- p. Data obtained from (public) social profiles (Facebook, LinkedIn and Twitter accounts, etc.)
- q. Other, namely:

Classification of the context involved in the breach:

The breach involves the personal data of **how many** persons?

- a. None, the data cannot be attributed to an individual
- b. Not yet established
- c. At least (number), but no more than(number) involved

Describe the group of people whose personal data were involved in the breach:

Circumstances of the data leak:

- a. Read only (an unauthorised third party was able to inspect (confidential) data. Processor still has the data in its possession.) – **Confidentiality is at risk**
- b. Copy (an unauthorised third party was able to copy data. The data are still in the possession of Processor.) – **Confidentiality is at risk**
- c. Alteration (an unauthorised third party was able to alter data in systems of the Processor – **Integrity is at risk**
- d. Removal or destruction (an unauthorised third party removed data from the systems of the Processor or destroyed data.) – **Availability is at risk**
- e. Theft – **Availability is at risk**
- f. Not yet known

Were the Personal Data made incomprehensible or inaccessible for unauthorised third parties, for example by encryption and hashing?

Yes

No

Partly, i.e.

If so, how were the Personal Data encrypted?

Did the breach involve persons from other EU Member States?

Yes

No

If so, which EU Member States:

Which security measures (technical and organisational) have been implemented to tackle the breach and to prevent further breaches?

Who can be contacted for more information on the breach?

Name of contact person of the Supplier:

E-mail:

Telephone number:

ANNEX 5 – QUESTIONNAIRE IN CASE OF USE OF CLOUD SERVICES

Good practices Cloud

Under Article 5, 1, f of the GDPR, the processing of personal data is only permitted if appropriate security of the personal data is guaranteed by taking appropriate **technical or organisational measures**, in such a way that they are protected, among other things, against **unauthorised or unlawful** processing and against **accidental loss, destruction or damage** (integrity and confidentiality). These measures must ensure an appropriate level of security, taking into account, on the one hand, the state of the art in this area and the costs of implementing the measures and, on the other hand, the nature of the data to be protected and the potential risks.

When drawing up this questionnaire, the starting point is the principle that the public cloud service provider may **not have access** to the information processed on the platform. This is achieved with confidential compute, where encryption ensures that the service provider does not have access to readable data and code in both the memory and the computing unit. This secure environment is also called an enclave

Type of data	Anonymously	Pseudonymized	Nominative
Cloud provider name			
Location storage data			

Access to the processed information by public cloud provider:

	Measure taken
Data in rest Data at rest* must be protected, decrypted only within the secure enclave, and re-encrypted before leaving the enclave.	
Data in transit "Data in transit" must be protected, decrypted only within a secure enclave, and re-encrypted before leaving the enclave.	
Others Information may not be transferred readably over cloud networks. The exchange of information with the cloud platform must be secured.	
Attestation of confidential computing of the public cloud platform Vooraleer de software processes sensitive information on the confidential computing platform, it must have sufficient guarantees that the platform offers the necessary guarantees for security. This is done by means of attestation of the confidential compute. The attestation must make it possible to verify that the execution environment is trusted and real, must be done in a reliable way and must also be secured. The attestation must be able to be performed independently of the public cloud service provider.	
Encryption tools and secrets Encryption keys and secrets are secured within the enclave and will never leave the enclave readable. Encryption keys and secrets are managed on a system that the public cloud service provider does not have access to.	

Means of authentication Authentication means should be treated the same as secrets. The public cloud service provider does not have access to the system that manages the authentication means or the system that performs the authentication. The public cloud service provider does not have logical access to the servers or the enclaves, even with their own authentication means. The cloud application uses multi-factor authentication (MFA)	
Authorization means The public cloud service provider does not have access to the system that manages the authorizations. Access management for the cloud application is done via Azure AD Link	
Deletion The public cloud service provider provides the necessary guarantees that data is effectively removed from the storage systems when the user instructs this and has this procedure regularly certified by an external party.	
Monitoring of technology used The user must enter into an agreement with the public cloud service provider that the user will be immediately informed of any vulnerabilities of the platform or parts thereof so that the user can take appropriate measures to limit the risk.	
Applicable regulations and disputes The contracts with the public cloud service provider must be declared under Belgian law or the law of another European country. Disputes related to the GDPR will be handled by the Belgian Data Protection Authority.	
Service level agreement The relationship with the public cloud service provider must include a service level agreement that provides sufficient guarantees that the public cloud service provider will respond appropriately to any threat that could impact the protection of the information.	
Backup Organizations that process personal health information must back up all personal health information and store it in a physically secure environment to ensure future availability. To protect confidentiality, encrypted backups of personal health information must be made.	