ADDENDUM TO SUPPLIER AGREEMENT ON DATA PROTECTION

Between

Jan Yperman ziekenhuis vzw
with registered office at Briekestraat 12, 8900 Ypres
lawfully represented for the present purposes by Mr Frederick Chanterie, Managing Director
Hereinafter referred to as '**the Hospital**'

And

[Name of
with registered [addres
lawfully represented for the present purposes by [name and
position]Hereinafter referred to as '**the Supplier**'

Hereinafter jointly referred to as '**the Parties**' WHEREAS

The Supplier provides services on behalf of the Hospital, as described in the Basic Agreement; these services entail the processing of personal data, and through the present Addendum, the parties wish to lay down the agreements concerning the processing of personal data within the framework of the services.

AND WHEREAS the Supplier is an expert in providing the supplies and/or services that are the subject of the Main Agreement, and the Supplier has the necessary resources to provide the supplies and/or services according to the best trade practices and can demonstrate this through relevant, reliable references.

NOW THEREFORE it is hereby agreed as follows:

1. CONCEPTUAL FRAMEWORK

11 For the application of the present 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 the free movement of such data, and repealing Directive 95/46/EC, with its amendments and the European implementing legislation;
- **Data Protection legislation**: the General Data Protection Regulation, other European regulations containing provisions relating to data protection and privacy, as well as applicable national data protection legislation and privacy in the Member States, together with its amendments and implementing acts, including approved codes of conduct applicable to the sector;
- **Personal data, Processing, Controller, Processor, Data Subject, Consent**: the definitions shall be as set out in the General Data Protection Regulation;
- **Basic agreement**: the agreement between the Hospital and the Supplier, appended as an Annex to the present processing agreement.

12 The Supplier provides supplies and/or services to the Hospital pursuant to and as defined in the Basic Agreement. The following qualification applies to the processing activities as defined in **Annex 1** to this Addendum:

- the Hospital determines the purpose and - in whole or in part - the means of processing, and is consequently the Controller;
- the Supplier performs the processing of personal data on behalf of the Hospital and is consequently a Processor.

2. SCOPE AND RELATIONSHIP WITH THE BASIC AGREEMENT

21 This Addendum constitutes 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 that the

Supplier performs in the context of processing activities as specified in **Annex 1**.

2.2 The provisions of this Addendum (and Annexes) shall take precedence over (any contrary) provisions on data protection and processing and confidentiality of data that may be contained in the Basic Agreement, and shall replace the same.

2.3 All costs to be incurred by the Supplier in order to comply with the requirements set out in this Addendum shall be deemed to have been included in the price specified in the Basic Agreement, unless otherwise provided in the Basic Agreement.

3. PROCESSING IN CONFORMITY WITH THE REGULATORY AND WRITTEN INSTRUCTIONS OF THE HOSPITAL

3.1 When processing personal data, the Parties shall comply with the Data Protection Legislation.

3.2 The Supplier shall process personal data solely on the basis of the written instructions of the Hospital, unilaterally determined by the Hospital, and as set out in **Annexes 1 and 2** to this Annex. If the written instructions are not clear, the Supplier shall notify the Hospital of the same in writing, following which, through mutual consultation, the instructions shall be clarified.

Except as otherwise provided in this Annex, the Supplier shall not process personal data for its own purposes or for those of third parties, or provide the personal data to third parties, or transfer them to a country located outside the European Union, without having received written instructions from the Hospital. Any processing carried out in accordance with the Hospital's instructions may also mean the (immediate) stoppage of processing.

If European or national regulations make it mandatory for the Supplier to carry out a particular processing, the Supplier shall notify the Hospital of such legal requirement before such processing, unless such regulation prohibits such notification for important grounds of public interest.

3.3 The Hospital shall provide instructions to the Supplier in accordance with the Data Protection Legislation, and warrants that all personal data entrusted to the Supplier were lawfully obtained 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.

4.2 In determining the measures, account shall be taken of the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

The measures include the following, wherever appropriate:

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

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 confirms that it shall at least implement the technical and organisational measures described in **Annex 2**, without prejudice to the instructions arising directly from the provisions of the Basic Agreement or the present Addendum, or such measures as are reasonably required for the Supplier's proper performance of its obligations.

4.3 The Supplier shall comply with the standards of approved codes of conduct and certification mechanisms as applicable within the sector.

The Hospital requires compliance with the ISO/IEC 27001 and 27002 Standards at all times during the processing of personal data. The Supplier shall preferably submit certification with regard to these standards. If the Supplier does not have ISO/ IEC 27001 and 27002 certification, the Hospital may accept other certificates, but the Supplier must always at least conform to the spirit of the ISO/ IEC 27001 and 27002 Standards during the performance of its work.

5. PROCESSING BY A SUBPROCESSOR OR EMPLOYEE

5.1 The Supplier shall ensure compliance with the provisions of the present Addendum by its representatives, agents, subcontractors and employees. The Supplier shall only share personal data of the Hospital with, or make it available to, its representatives, agents, subcontractors and employees who are directly involved in the performance of the Basic Agreement, on a need-to-know basis.

By extension, the Supplier warrants that:

- the persons authorised to process personal data have either contractually undertaken to observe confidentiality, or are bound by an appropriate legal obligation of confidentiality;
- measures have been taken to ensure that every natural person acting under its authority who has access to the personal data, only processes them (except as otherwise provided in this Addendum) on behalf of the Hospital, unless it is obliged to process the same under European or national regulations.

5.2 At the time of signing the present Addendum in **Annex 1**, the Supplier shall make the disclosure concerning each of the Subprocessors or categories of Subprocessors relied upon by it and the Hospital, by signing the present Addendum, and granting its general consent to the same.

The Supplier shall notify any new Subprocessors or new category of Subprocessors to the Hospital by means of **Annex 5**.
If, within 14 days of receipt of the Supplier's notification, the Hospital expresses any objection (founded on reasonable grounds) regarding the
proposed new Subprocessor, the Supplier shall not
transfer personal data from the Hospital to the proposed
Subprocessor, except with the prior written and explicit consent of the Hospital.
In case of force majeure or technical problems, the Supplier may
rely upon a new Subprocessor without prior notice to the Hospital. The Hospital reserves the right to oppose one or more Subprocessors at any time.

5.3 If the Subprocessor fails to comply with its data protection obligations, the Supplier shall remain fully liable to the Hospital for compliance with the Subprocessor's obligations.

6. TRANSFERS TO A COUNTRY LOCATED OUTSIDE THE EUROPEAN ECONOMIC AREA

6.1 If personal data is transferred to a country or organisation outside the European Economic Area, the Supplier shall comply with the safeguards of Chapter 5 of the GDPR, and provide appropriate safeguards. The
Supplier shall notify the Hospital concerning every transfer made outside the European Economic Area:

- The country to which the transfer is made
- The transfer tool
- The analysis and assessment concerning additional measures
  that must be taken in order to implement the transfer (Transfer Impact Assessment (TIA)).

6.2 In case the Supplier transfers 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, as well as additional measures to be implemented by the Supplier. The Supplier shall provide such assessment (Transfer Impact Assessment) on
first request from the Hospital.

6.3 If the concrete transfer tool as per Section 45 to 49 of the GDPR is not effective, and no additional measures are taken to ensure the

level of data protection as set out in the GDPR, it shall not be permissible for the Supplier to transfer the personal data
outside the European Economic Area, except where the Hospital has given its prior written consent.

6.4 This clause also covers transfers if any made by the Subprocessors relied on by the Supplier to process personal data on behalf of the Hospital.

7. PROVIDING ASSISTANCE WITH THE OBLIGATIONS RELATING TO 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 undertakes to provide assistance
to the Hospital with regard to the Hospital's responsibility 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 by the Hospital of a personal data breach to the supervisory authority;
- communication by the Hospital of a breach related to personal data of the data subject, to the data subject;
- the conduct of a data protection impact assessment (DPIA);
- the prior consultation by the Hospital of the supervisory authority if
  the
  data protection impact assessment (DPIA) shows that the
  processing would pose a high risk in case the Hospital does not take measures to mitigate the risk.

The time and resources spent by the Supplier in providing the assistance shall be for the Supplier's own account, except in case of
provision to the contrary in the Basic Agreement.

In line with Clause 7. 1., the Supplier shall notify the Hospital
in detail and immediately concerning a (suspected) personal data breach, as well as concerning every data breach (including at the Subprocessor's premises) as soon as the Supplier becomes aware of the same. The notification shall be made
in such a manner that the Hospital can meet its

legal obligations as a controller under the
Data protection legislation. The Supplier shall indemnify the Hospital in accordance with Clause 10.2.

The Supplier shall use the notification form provided in **Annex 4** to make the notification. The Supplier shall also provide assistance in the investigation, mitigation and remedy of an infringement related to processing of
personal data. This shall include assistance with a view to documenting measures such as data protection by design and by default settings.

7.2 The Supplier shall immediately notify the Hospital of any
complaint, allegation or request made (even if from a regulator) concerning the processing of personal data by the
Supplier. The Supplier shall provide all the necessary cooperation and support that the Hospital may reasonably expect in relation to
such complaint, allegation or request, among other things through the
provision of comprehensive information concerning such complaint, allegation or request, together with a copy of the personal data relating to the data subject, that may be in the Supplier's possession.

8. PROVISION OF ASSISTANCE IN CONNECTION WITH THE REQUESTS OF DATA SUBJECTS

8.1 Taking into account the nature of the processing, the Supplier shall assist the Hospital through appropriate technical and organisational measures in connection with the fulfilment of the Hospital's duty to
respond to requests to exercise the rights of data subjects, as stipulated in the Data Protection Act.

This implies, among other things:

- that the Supplier will provide all the
  personal data, within the (reasonable) time requested by the Hospital, in any case including full details and copies of the complaint, notification or request along with any
  personal data concerning the data subject, that it may have in its possession;
- that the Supplier implements such technical and organisational measures that allow the Hospital to effectively and in a timely manner
  respond to relevant complaints, notifications or requests.

The time and resources spent by the Supplier in providing the assistance shall be for the Supplier's own account, except in case of
provision to the contrary in the Basic Agreement.

8.2 In line with Clause 7. 1., the Supplier undertakes to
immediately notify the Hospital if it receives, from a data subject (or third party acting on behalf of a data subject) one of the following requests:

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

The Supplier shall not itself respond to requests and enquiries from data subjects, except in the case of written agreements if any to the contrary between the Hospital and the Supplier.

9. RIGHT TO AUDIT BY THE HOSPITAL

9.1 The Hospital shall always have the right to verify the Supplier's compliance with this Addendum. The Supplier shall provide the Hospital with comprehensive
information as may be required to demonstrate compliance with obligations under the Data Protection Act. The
Supplier shall enable audits, including inspections by the Hospital or an
auditor authorised by the Hospital, and shall contribute to the same. The Supplier shall cooperate fully with regard to any such audit and shall, at the request of the Hospital, provide evidence of compliance with
its obligations under this Annex.

9.2 The Supplier shall notify the Hospital within a reasonable time if, in its opinion, an instruction violates the
Data Protection Act.

10. LIABILITY

10.1 Each of the parties shall be responsible and liable for their own actions. The liability laid down under the present clause refers only to liability arising from a breach of the Data Protection Act and this Addendum.

10.2 The Supplier shall compensate and indemnify the Hospital in respect of all claims, lawsuits, third-party claims as well as for all damages and losses (including fines imposed by the Data Protection Authority) that directly or indirectly arise from the processing of personal data in case the processing did not comply with the obligations laid down under the Data Protection Act, that are specifically aimed at processors, or if the processing was carried out otherwise than in conformity with the legitimate instructions of the Hospital, or in violation thereof.

10.3 The Parties shall ensure adequate coverage of their liability.

11. END OF THE AGREEMENT

11.1 If the Supplier fails to properly fulfil its obligations under this Addendum and fails to take appropriate action within a maximum period of two months, the Hospital may - without prejudice to other grounds of termination as provided for in the Basic Agreement - immediately terminate the Basic Agreement, after the aforementioned period of two months and/or discontinue the processing operation.

11.2 This agreement and the Basic Agreement together form a whole, and shall therefore have the same fate as the Basic Agreement. In case the Basic Agreement comes to an end, the provisions of this Addendum shall nevertheless continue to apply, insofar as necessary, to the fulfilment of obligations under the Data Protection Act.

11.3 Immediately upon (any) termination or expiry of the Basic Agreement, or after the expiry of the retention period, the Supplier will - according to the choice of the Hospital - return the personal data to the Hospital and/or fully or irreversibly delete the personal data, and

also delete existing copies. In case the Hospital chooses to delete the personal data, the Supplier shall, on the written request of the Hospital, prove that the deletion has actually happened.

The Supplier may deviate from the first paragraph provided the storage of the personal data is required by European or national legislation, and the Supplier has notified the Hospital of such obligation.

12. FINAL PROVISIONS

12.1 In case of the nullity or voidability of one or more provisions of this Annex, the remaining provisions shall remain in full force and effect.

12.2 This Addendum is governed by Belgian law. Disputes shall be submitted to the tribunals/courts in the judicial district of Ypres, which shall have exclusive territorial jurisdiction.

Thus agreed and drawn up at [municipality] on [date].

Frederik Chanterie Managing Director	Maarten Crappé Director, Administration and Finance
Mr Hans Feys Hoofdarts	[Name] Head of Medical department

VZW Jan Yperman Ziekenhuis

[Name] [Position]	[Name] [Position]

Supplier

Annexes

- Annex 1: The processing operation and instructions as determined by the Hospital
- Annex 2: Other instructions for processing personal data, and minimum security measures
- Annex 3: Confidentiality obligations
- Annex 4: Model data breach notification form
- Annex 5: Model form for adjustments to Annex I after concluding the processing agreement

ANNEX 1

THE PROCESSING OPERATIONS AND INSTRUCTIONS AS DETERMINED BY THE HOSPITAL

Introductory note

This Annex describes the specific processing operations by the Supplier that the Hospital commissions at the time of concluding the
Basic Agreement, or upon signing the Annex.

- **The purpose of the processing of personal data**

The processing of personal data by the Supplier shall take place in the context of the performance of the Basic Agreement.

Description of the supplies/services under the Basic Agreement and the nature and purpose of the processing of personal data under the provision of supplies/services:

[To be completed by the Supplier: description of the services under the Basic Agreement and the nature and purpose of the processing of personal data in the context of the services].

- **The categories of personal data that the Hospital allows to be processed by the Supplier (indicate what applies and complete if necessary):**
  - contact details
  - financial data
  - invoice data
  - wage data
  - health data
  - marketing data
  - data concerning the Hospital's use of the Supplier's services and associated products
  - other (to be specified):
    ……

L. The categories of data subjects whose personal data are processed (indicate what applies and complete if necessary):

- **Hospital patients**
- confidential advisers, representatives and contact persons of the Hospital's patients
- caregivers of the Hospital's patients
- Hospital staff members
- other (to be specified):

  ……

M. The processing of personal data (indicate what applies and complete if necessary):

The Hospital hereby gives the following instructions for the processing of the personal data (without prejudice to any instructions arising directly from the provisions of the Basic Agreement or this Addendum, or reasonably required for the proper performance by the Supplier of its obligations):

- Consulting personal data

  These are services provided by the Supplier where personal data of the Hospital can be viewed by employees or by subcontractors of the Supplier, including but not limited to, service desk Services, (remote) monitoring Services, system management Services, technical application management, vulnerability scanning Services, reporting Services in governance and software asset management Services, the provision of support (helpdesk, remote monitoring, etc.).

- Storing personal data

  These are services provided by the Supplier in which the Hospital's personal data is stored in a storage system provided by the Supplier including but not limited to cloud storage Services, cloud back up Services, file Services, directory Services, managed file transfer, mail & calendaring and logfile processing.

- Forwarding personal data

  These are services of the Supplier in which personal data of the Hospital are sent from, to or between applications on a platform managed by the Supplier, such as, but not limited to, LAN Services, Wide Area Network Services, data centre interconnectivity services, Loadbalancing, SAN switch interconnects and

Services provided over the Voice over Internet Protocol (VoIP).

- Updating or modifying personal data
  These are services of the Supplier whereby personal data of the Hospital can be modified manually as well as
  in an automated manner, such as in an automated job flow supported by a job scheduling system.

- Software testing
  These are services of the Supplier involving databases of the
  Hospital that contain personal data (personal data that are not
  anonymised), and are used outside the production environment (in test, acceptance, etc.) as part of the testing process of the Hospital software
  application.

- Other: …….

The personal data will not be used by the Supplier under any circumstances, and shall not under any circumstances be used for purposes other than those described in the Addendum and this Annex. This prohibition also applies to mere internal (re)use by the Supplier. Deviations from the same may only be made with the prior consent of the Hospital, attached as an annex to the
processing agreement.

V. The retention periods of the (different categories) of personal data:

The Supplier shall retain the processed personal data in an adequately secure manner for the period necessary to execute the written
instructions of the Hospital, and in conformity with the provisions as agreed in the Basic Agreement.

In case of personal data that form part of patient records, a minimum retention period of 30 years shall always apply to the Hospital.

VI. List of Subprocessors:

Name of subprocessor	Contact DPO	Place of processing	Nature of processing

VII. List of transfers to third countries:

Data exporter	Data importer	Country in which personal data are processed	Transfer tool (Standard Contractual Clauses, Binding Corporate Rules, etc.) and additional measures (if necessary) (*)

(*) if the Hospital is a data exporter and the European Commission's European Standard Contractual Clauses (ESCC's) are invoked,
these ESCC's shall be appended as Annex 5 to the processing agreement.

VIII. The Data Protection Officer or other responsible contact person for data protection and processing (please complete):

For the Hospital

Name: Mr Niels Vermeersch

Contact details: dpo@yperman.net

For the Supplier

Name: [Name]

Contact details: [e- mail].

ANNEX 2

OTHER INSTRUCTIONS FOR PROCESSING PERSONAL DATA, AND MINIMUM SECURITY MEASURES

The Hospital requires compliance with the ISO/IEC 27001 and 27002 Standards at all times during the processing of personal data. The
Supplier should preferably submit certification for these standards. If the Supplier does not have ISO/IEC 27001 and 27002 certification, the
Hospital may accept other certificates, but the Supplier must always at least conform to the spirit of the ISO/IEC 27001 and 27002 Standards
during the performance of its work.

The Supplier additionally confirms that it shall at least implement the following technical and organisational measures, without prejudice to the instructions that may
arise directly from the provisions of the Basic Agreement or this Addendum, or that are reasonably required for the proper performance of its obligations.

If the Supplier cooperates with Subprocessors, the Supplier warrants that each of the Subprocessors shall operate in accordance with the same standards and shall fulfil the same minimum requirements.

The Supplier confirms that it has taken cognisance of the "Code of Conduct on Information Security for Suppliers" and the "IT - Requirements for PCs",
Server software, medical devices and peripherals" as available on the Hospital's website.

The Hospital may - as part of its information security policy - request that a Supplier Information Security Assessment should be
completed by the Supplier.

MINIMAL MEASURES FOR THE SUPPLIER AND ITS SUBPROCESSORS:

1. CONSULTING PERSONAL DATA AT THE HOSPITAL

For processing activities in which personal data do not leave the Hospital, the following minimum measures shall have cumulative application:

11. Personal data may only be consulted by the in-house staff of the

Supplier, to the extent strictly necessary for the performance of the task as defined in the Basic Agreement.

12. On the simple request of the Hospital, the Supplier shall provide an up-to-date list of persons who, for the performance of their task, require access to the systems. The grounds for requesting access rights shall also be stated therein. Changes in this list shall immediately be notified by the Supplier to the Hospital.

13. The Supplier shall ensure that each of the persons to be granted access shall be subject to the obligation to maintain confidentiality and discretion as drawn up by the Hospital (see **Annex 3**).

14. Each of the individuals who will have access to sensitive data at the Hospital should have received adequate information as well as training from the Supplier with regard to obligations and responsibilities during the (potential) consultation of personal data. The Hospital may additionally require that a training course, as provided by the Hospital should be followed.

2. STORAGE OF PERSONAL DATA OUTSIDE THE HOSPITAL

For processing activities in which personal data leave the Hospital and are retained by the Supplier (or its Subprocessor), the following shall apply - in addition to the aforementioned obligations - cumulatively, along with the following obligations:

21. By concluding this Addendum, the Supplier declares that it has the following documents in its possession.

211. An implemented Information Security Plan (Information Security Management System) together with the confirmation that the policy was approved by the highest hierarchy and various responsible persons.

212. An implemented Back-up and Disaster Recovery Plan that specifies at least the following:

- which back-up mechanisms will be used and whether or not they are adequate;

- which recovery tests will be used and whether or not the reporting thereof is available.

213. An implemented Identity and Access management (IAM) policy that at least supports the following principles:
    - clearly defined, role-based access rights;
    - withdrawal of access at the end of cooperation;
    - strong Authentication;
    - full logging of IAM and data access.

214. An implemented Incident Management Procedure. This shall at least describe how consequences of incidents for the data of the Hospital shall be limited, the steps to be taken in case of discovery of a security incident, and the persons who shall be responsible for addressing the incident to restore a healthy state.

22. The Supplier confirms compliance with the following technical and organisational requirements:

221. That the data obtained from or via the Hospital may not leave the borders of the European Economic Area. If they do leave the said borders, the Supplier must submit the necessary guarantees proving that the transfer complies with Chapter V of the General Data Protection Regulation (Transfer of personal data to third countries or to international organisations).

222. That the networks over which data is transmitted (fixed or wireless, from, to or between applications, or via a platform managed by the Supplier, such as, among others, but not limited to LAN services, WAN services, data centre, interconnectivity services, load balancing, SAN (Storage Area Network Switch) switch interconnects and services provided over the VoIP) are secured according to the rules of good practice and applicable standards, and that techniques appropriate for the transmission of sensitive data are used.

223. That the hardware (including Virtual Machine) has been equipped with adequate monitoring mechanisms and security systems to prevent and analyse data breaches.

224. That the IT systems used have been installed in accordance with their classification in identified and protected premises,
to which access is restricted.

225. That all server stations are equipped with prevention and detection mechanisms, as well as means to contain virus and other malware, and further that the server stations
have undergone a hardening process.

226. That all server stations have been equipped with an (implemented and documented) patch management process.

227. That for all server stations, patches are tested in an acceptance environment before the same are deployed.

228. That the systems are subjected to a penetration test and/or ethical hacking at least once a year.

23. The Supplier warrants that it can prove the implementation of these measures through (external) reporting, drawn up at least once every 3 years, according to a precisely defined
pattern. At the time of concluding the Agreement, the Hospital may request the latest (external) reporting or a document indicating by whom the reporting was made, when, and on what basis,
from the Supplier.

24. The Supplier may never modify the
personal data of the Hospital - either in a manual or in an
automated manner - except in cases where the Hospital has given its explicit consent

25. The Supplier warrants that in case of termination or expiry (if any) of the Basic Agreement, or on expiry of the retention periods
as provided for in Clause V. of **Annex I**, it shall, at the Hospital's request and option, securely return all data (in a format that is readable by the Hospital)

and shall destroy the same at its end, including all media used for data storage.

ANNEX 3

CONFIDENTIALITY OBLIGATIONS

The Supplier and its appointees shall, during their presence on the Customer's premises always fully comply with all rules and regulations applicable within the Customer's organisation, in particular, those relating to
safety, health and hygiene.

They undertake, both during the performance of their work for the Customer, as well as after the same comes to an end, to treat any information that may come to their knowledge which is or may be of a confidential nature, and which is directly or indirectly related to the activities of, or within the Customer organisation (such as all information about patients, data relating to personnel and
personnel-related matters, reports, business information in the widest sense of the term, data of a medical - technical, technical, financial or commercial nature, etc.) as classified information.

This shall also include all confidential information communicated by or relating to persons or institutions with whom they have come into contact in any manner during their presence on the Customer's premises.

If, within the scope of the operation, access is granted to the electronic
systems of the Hospital, in particular the system for the management of the electronic patient records, the Supplier or its appointee shall always fully comply with all the regulations, rules and procedures that apply within the Customer organisation regarding the use of these systems.

This means, among other things, that

- only personal login details that have been provided by the Hospital may be used to access the system;
- The personal password must be kept strictly secret;
- Consultation and possibly modification of (patient) data is only permissible within the framework of the agreed task;
- The Supplier shall be responsible and liable for everything that happens during the log-ins of its appointees;
  The Supplier shall be responsible for notifying its
  appointees that the Customer maintains logs of all actions carried out by its appointees.

Hospital contact details (contactable 24/7):
Department: DPO
E-mail: dpo@yperman.net

Date:
Company name:
Address:
Postcode:
VAT number:
Who identified the breach?
Name:
Job title:
When was the breach detected?
Date:
Time:
Describe the security incident in which the personal data security breach occurred:
When did the breach take place?
a. On (date + time)
b. Between (date + time) and (date + time)
c. Has not yet been established
d. There was an anonymous disclosure by a third party
Establish the context of the data involved in the breach:

Classification of data:
a. None, the data is not traceable to an individual
b. Name, address and residence details
c. Telephone numbers
d. E-mail addresses, Facebook ID's, Twitter ID's, etc.
e. User names, passwords or other login details, customer numbers
f. Financial data: account numbers, credit card numbers
g. National registry number
h. Copies of identity documents
i. Gender, date of birth, and/or age
j. Data on a person's religion or belief, race, political affiliation or membership of a trade union
k. Data about a person's health or sexual orientation
l. Personal data relating to criminal convictions and offences or personal data on unlawful or objectionable behaviour in connection with a prohibition imposed as a result of such behaviour
m. Data on a person'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, living situation, interests), demographic characteristics (age, gender, nationality, occupation, education)
p. Data obtained from (public) social profiles (Facebook, Linked In and Twitter accounts, etc.)
q. Other data, namely:
Classification of the context of the data involved in the breach:
What is the number of individuals whose personal data is involved in the breach?
a. None, the data is not traceable to an individual
b. Not yet determined
c. At least ..... (number), but no more than ……..(number) of data subjects
Describe the group of people whose personal data is affected by the breach:
Circumstances of the data breach:

a. Read only (an unauthorised third party has been able to view (confidential) data. The processor still retains possession of the data) - **Confidentiality is at risk**
b. Copying (an unauthorised third party has been able to copy data. The data is also still in the possession of the Processor.) - **Confidentiality is at risk**
c. Modifying (a non-authorised third party has modified data, or can modify the same, in the systems of the Processor) - **Integrity is at risk**
d. Deletion or destruction (a non-authorised third party has deleted data from Processor's systems or destroyed data) - **Availability is at risk**
e. Theft - **Availability is at risk**
f. Not yet known
Are the personal data rendered unintelligible or inaccessible to unauthorised third parties, e.g. by encryption and hashing?
Yes
No
Partial, namely
If so, in what way are the personal data encrypted:
Does the infringement relate to persons from other EU countries?
Yes
No
If so, which EU countries:
What security measures (technical and organisational) have been taken to address the breach and prevent further breaches?

Who can be contacted for more information concerning the breach?
Name of the contact person of the Supplier:
E-mail:
Telephone number:

ANNEX 5

MODEL FORM FOR ADJUSTMENTS TO ANNEX 1 AFTER CONCLUDING THE PROCESSING AGREEMENT

If the Parties wish to provide for certain aspects differently or more specifically, or to add certain matters after the conclusion of the
processing agreement, the same should be explicitly agreed with the Hospital through this form.

The amendments to this Annex shall only be valid and enforceable if this Annex has been signed and dated by both parties.

Clause	Text that is (possibly) cancelled	Replaced or added text	Reason

Thus agreed and drawn up at [municipality] on [date].

Frederik Chanterie Managing Director	Maarten Crappé Director, Administration and Finance
Mr Hans Feys Hoofdarts	[Name] Head of Medical department

VZW Jan Yperman Ziekenhuis

[Name] [Position]	[Name] [Position]

Supplier