**DATa PROCESSING AGREEMENT**

**addendum to the basic agreement d.d. xxx**

**Between**

UZ Leuven

with registered office at Herestraat 49, 3000 Leuven

legally represented by its CEO

Hereinafter referred to as **‘the Principal’**

**And**

**‘the Contractor’**

Hereinafter jointly referred to as **‘the Parties’**

**Considering that**

* The Contractor will provide supplies and/or services for the Principal, as described in the Basic Agreement, whereby the Contractor will process personal data and the Parties, by means of this Addendum, wish to establish the arrangements for this processing of personal data
* The Contractor is an expert in providing supplies and/or services that are the subject of the Basic Agreement, the Contractor has the means and resources to provide supplies and/or services as an expert and is able to demonstrate this by means of relevant and reliable references;

**the following has been agreed**

# Definitions

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

### **General Data Protection Regulation (GDPR)**: 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 Principal and the Contractor for performance of work, provision of services or products, to which this data processing agreement is an addendum.

## The Contractor shall provide supplies and/or services to the Principal on the basis of, and as defined in, the Basic Agreement. For the processing activities as specified in **Annex I** to this Addendum, the following qualification shall apply:

## the Principal shall determine the purpose and at least the essential means of processing and shall consequently be controller;

## the Contractor shall carry out the processing of personal data on behalf of and according to the instructions of the Principal, and shall consequently be processor.

# Scope and relationship to the Basic Agreement

## This Addendum shall form an integral part of the Basic Agreement concluded between the Principal and the Contractor. The provisions of this Addendum shall apply in full to all processing of personal data performed by the Contractor in the context of the implementation of the processing activities specified in **Annex 1**.

## The provisions of this Addendum (and Annexes) shall take priority over the (possible contrary) provisions concerning data protection and processing and confidentiality of data in the Basic Agreement, and shall replace these provisions.

## Any and all costs which the Contractor incurs to fulfil the requirements as specified in this Addendum are considered to be included in the fee which was agreed upon in the Basic Agreement.

# Processing in accordance with the regulations and the written instructions of the Principal

## When processing personal data, the Parties shall act in accordance with the Data Protection Legislation.

## The Contractor shall process the personal data exclusively on the basis of the written instructions of the Principal, unilaterally determined by the Principal and as specified in **Annexes 1** and **2** to this Addendum. If the written instructions are not clear, the Contractor shall notify the Principal of this in writing, whereupon the instructions shall be clarified by mutual agreement.

## Unless otherwise stipulated in this Addendum, the Contractor 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 Economic Area without having received a written instruction to do so from the Principal. Processing in accordance with the instructions of the Principal may also mean that the processing must be stopped (immediately).

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

## The Principal shall give instructions to the Contractor in accordance with the Data Protection Legislation and shall ensure that all personal data entrusted to the Contractor have been obtained lawfully and can be processed under the Basic Agreement.

## The Contractor shall inform the Principal immediately if, in its opinion, an instruction breaches the Data Protection Legislation.

# Appropriate technical and organisational measures

## The Parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in accordance with article 32 GDPR.

## 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 risks 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.

## 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, unauthorized disclosure of, or unauthorized access to personal data transmitted, stored or otherwise processed.

## The Contractor commits to taking the technical and organisational measures as described in **Annex 2** at a minimum, without prejudice to the instructions directly arising from the stipulations in the Basic Agreement or this Addendum or which are reasonably required for the Contractor to carry out its obligations correctly.

## The Contractor shall adhere to the standards of approved codes of conduct and certification mechanisms as applicable within the sector.

## The Principal requires that, when processing personal data, the Contractor shall at any time and always operate in accordance with the ISO/IEC 27001 and 27002 Standards. The Contractor preferably provides certification for these standards. If the Contractor does not have the ISO/IEC 27001 and 27002 certification, the Principal can accept other certification, but the Contractor shall at least work in accordance with the spirit of the ISO/IEC 27001 and 27002 Standards.

Only for the tasks whereby the Principal itself gives access to the Contractor for a limited amount of time to certain personal data and this processing occurs in the presence/under the supervision of the Principal’s appointee (for example in the context of tasks IT-support for maintenance or incident,…), the Contractor’s obligation to provide certification is not applicable. However, all other instructions as described in **Annex 2**, as well as the commitments in the context of confidentiality as described in **Annex 3**, remain applicable in such case.

# Processing by a ‘Sub-processor’ or employee

## The Contractor shall ensure that its representatives, agents, subcontractors and employees comply with the provisions of this Addendum. The Contractor will only disclose or make available the personal data of the Principal to its representatives, agents, subcontractors and employees who are directly involved in the performance of the Basic Agreement, on a strict need-to-know basis.

## The Contractor shall ensure, in line with this:

## that persons authorised to process personal data have contractually 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 Principal, unless required to process them by European or national legislation.

## When this Addendum is signed, the Contractor communicates in **Annex 1** each Sub-processor that processes personal data for the Contractor, and the Principal authorizes this by its signature. The Contractor will communicate each and every new Sub-processor to the Principal by means of **Annex 5**. The Principal reserves the right to object to one or more Sub-processors at any time. If the Principal informs the Contractor within 14 days after receiving notification from the Contractor of any objection (on reasonable grounds) to the proposed addition or replacement, the Contractor will not provide or disclose the personal data of the Principal to the proposed Sub-processor, except with the prior written and explicit consent of the Principal.

## If the Contractor engages a Sub-processor, it will enter into a written agreement with this Sub-processor which stipulates the same or equivalent obligations as those of the Contractor as set out in this Addendum and meets the requirements of article 28 GDPR. If the Sub-processor fails to comply with its data protection obligations, the Contractor shall remain fully liable in relation to the Principal for complying with the Sub-processor’s obligations.

# Provision of assistance with respect to the obligations regarding the data protection policy of the Principal

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

## the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk;

## the notification by the Principal of a personal data breach to the supervisory authority;

## the communication by the Principal of a personal data breach to the data subject;

## carrying out a data protection impact assessment;

## the consultation by the Principal 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 Principal to mitigate the risk.

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

## Pursuant to Article 6.1, the Contractor shall inform the Principal 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 Contractor has become aware of this. The notification shall take place in such a way that the Principal can fulfil in time its legal obligations as controller under the Data Protection Legislation. The Contractor shall indemnify the Principal in accordance with Article 9.2.

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

## The Contractor shall notify the Principal immediately of any complaint, accusation or request made (including if it comes from a regulator) with regard to the processing of personal data on behalf of the Principal. The Contractor shall offer all necessary cooperation and support that the Principal 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 Contractor.

# Transfers outside the European Economic Area

## If personal data is being transferred to a third country or to an organisation outside the European Economic Area, the Contractor shall guarantee to abide to chapter 5 GDPR and to take appropriate safeguards.

## For any transfer outside the European Economic Area, the Contractor shall inform the Principal about:

## The third country of the transfer

## The transfer tool

## The analysis and assessment regarding the additional measures to be taken to carry out the third country transfer

## If the Contractor will process or have the personal data processed outside the European Economic Area, the Principal may request the assessment of the law and/or practices in force of the third country from the Contractor (Transfer Impact Assessment).

## If the specific transfer tool of art. 45 to 49 GDPR is not effective and no additional measures are taken to safeguard the level of data protection set out in the GDPR, the Contractor is not allowed to transfer the personal data outside the European Economic Area, except when the Principal has given its prior written consent to do so.

## This article also applies to any transfers made by the Sub-processors used by the Contractor to process personal data on behalf of the Principal.

# Provision of assistance for requests by the data subjects

## Taking into account the nature of the processing, the Contractor shall provide the Principal with assistance by means of appropriate technical and organisational measures in fulfilling the Principal’s obligation to respond to requests to exercise the rights of the data subjects, as specified in the Data Protection Legislation.

##

## This implies, inter alia:

* + that the Contractor provides all the personal data requested by the Principal within the (reasonable) period of time requested by the Principal, 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 Contractor implements technical and organisational measures that permit the Principal to reply effectively and in a timely manner to relevant complaints, communications or requests.

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

## Pursuant to Article 7.1, the Contractor shall undertake to inform the Principal 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 Principal under the Data Protection Legislation.

The Contractor itself shall not reply to the requests and applications by the data subjects, unless there are any written agreements to the contrary between the Principal and the Contractor.

# Right of audit by the Principal

## The Principal shall have the right at any time to check compliance by the Contractor with this Addendum. The Contractor shall make all information available to the Principal which is needed to demonstrate compliance with the obligations under the Data Protection Legislation. The Contractor shall make audits possible, including inspections, by the Principal or an auditor authorized by the Principal, and shall contribute to them. The Contractor shall grant full cooperation with regard to such an audit and, at the request of the Principal, shall supply evidence of compliance with its obligations under this Addendum.

# Liability

## 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.

## The Contractor shall reimburse and indemnify the Principal 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 Principal.

## The Parties shall ensure sufficient cover of their liability.

# End of the agreement

## If the Contractor 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 Principal – 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.

## This Addendum 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.

## Immediately on (no matter which) termination or expiry of the Basic Agreement or after the expiry of the storage period, the Contractor – at the discretion of the Principal – shall return the personal data to the Principal and/or irrevocably erase the personal data entirely and remove existing copies. If the Principal opts for the removal of the personal data, the Contractor shall demonstrate to the Principal, on written request, that the removal has in fact occurred.

## The Contractor may derogate from paragraph 1 if the storage of the personal data is required under European or national legislation and the Contractor has informed the Principal of this obligation.

# Final provisions

## In the event of nullity or voidability of one or more provisions of this Addendum, the other provisions shall remain in full force.

## This Addendum shall be subject to Belgian law. Disputes shall be brought before the tribunals/courts in the judicial district of Leuven, which shall have exclusive territorial jurisdiction.

\* \*

\*

Agreed and signed in duplicate in ………………………………………….. on …………………………………….. .

**The Principal** **The Contractor**

***Annexes***

Annex 1: The processing assignment and instructions as determined by the Principal

Annex 2: Additional instructions for the processing of personal data and minimum

security measures

Annex 3: Obligations in the context of confidentiality

Annex 4: Sample form for reporting data breaches

Annex 5:Sample form for changes to Annex 1 after the processing agreement is concluded

**Annex 1**

**The processing assignment and instructions as determined by the Principal**

***Introductory remark***

*This Annex describes the specific processing operations carried out by the Contractor as commissioned by the Principal at the time the Basic Agreement was concluded or the Addendum was signed.*

1. **The purpose of processing personal data**

The processing of personal data by the Contractor takes place in the context of implementing the Basic Agreement.

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

1. **The categories of personal data processed by the Contractor on the Principal’s assignment (indicate which apply and supplement where necessary):**
* contact data
* financial data
* invoice data
* wage data
* health data
* marketing data
* data concerning the Principal's use of the Contractor's services and accompanying products
* other (please specify):

…………………………………………………………………………………………………

1. **The categories of persons involved whose personal data is to be processed (indicate which apply and supplement where necessary):**
* the Principal's patients
* confidants, representatives and contacts of the Principal's patients
* the Principal's patients' carers
* the Principal's members of staff
* other (please specify):

…………………………………………………………………………………………………

1. **The processing of the personal data (indicate which apply and supplement where necessary):**

The Principal hereby issues the following instructions for processing the personal data (without prejudice to the instructions directly arising from the stipulations in the Basic Agreement or the Addendum or which are reasonably required for the Contractor to carry out its obligations correctly):

* Consult personal data
* Store personal data
* Transfer of personal data
* Change or update personal data
* Test software
* Providing support
* Other: …………………………………..

**On no account shall the personal data be used by the Contractor in any circumstances for purposes other than as described in this Annex.** This restriction also applies to solely internal use or re-use by the Contractor. Exceptions to this can only be made where prior permission from the Principal has been added as an annex to the processing agreement.

1. **The retention periods for the (different categories of) personal data:**

The Contractor will store the personal data processed in an adequately secure manner during the period necessary to carry out the Principal's written instructions and in accordance with the provisions agreed in the Basic Agreement.

Where this concerns personal data forming part of a patient record, a minimum retention period of 30 years will always apply.

1. **List of Sub-processors that process personal data for the Contractor for the purposes of implementing the Basic Agreement between the Principal and the Contractor (please specify in the following table):**

|  |  |  |
| --- | --- | --- |
| **Name Sub-processor** | **Address** | **Services that are performed by Sub-processor** |
|  |  |  |
|  |  |  |
|  |  |  |

1. **List of transfers of personal data outside the European Economic Area, including transfers of Sub-processor (please specify in the following table):**

|  |  |  |  |
| --- | --- | --- | --- |
| **Exporter** | **Importer** | **Country where the personal data will be processed** | **Transfer tool and supplementary measures (if applicable)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **The Data Protection Officer or other contacts responsible for data protection and processing (to be completed):**

**For the Principal**

Name: DPO UZ LEUVEN – 016 33 22 11

 Contact details: GDPR@UZLeuven.be

 **For the Contractor**

Name:

 Contact details:

**Annex 2**

**Additional instructions for the processing of personal data and minimum security measures**

1. The Principal requires that all actions taken when processing personal data are in compliance with the ISO/IEC 27001 and 27002 Standards. The Contractor will preferably present its certification for these standards. Should the Contractor not possess ISO/IEC 27001 and 27002 certification, the Principal may accept other equivalent certificates, but the Contractor should work at least within the spirit of the ISO/IEC 27001 and 27002 Standards at all times.
2. The Contractor also commits to taking the below-mentioned technical and organisational measures at a minimum, without prejudice to the instructions directly arising from the stipulations in the Basic Agreement or the Addendum or which are reasonably required for the Contractor to carry out its obligations correctly.

Where the Contractor is working with Sub-processors, the Contractor guarantees that each of the Sub-processors will work in accordance with the same standards and meet the same minimum conditions.

**Minimum measures for Contractors and their Sub-processors:**

**1. Consulting personal data within and outside UZ Leuven**

For processing whereby personal data does not leave UZ Leuven, the following minimum measures will apply cumulatively:

* 1. The personal data can only be consulted by the Contractor's own staff, and only insofar as this is strictly necessary to carry out the assignment described in the Basic Agreement.
	2. The Contractor will supply, at the Principal's request, a current list of individuals for whom access to the systems is necessary in order to carry out their assignment. This will also explain the reason for the request for access rights. Any changes to this list will be immediately communicated to the Principal by the Contractor.
	3. Each individual granted access will be subjected by the Contractor to the duty of confidentiality and discretion as drawn up by the Principal (see **Annex 3**).
	4. Each individual granted access to the Principal's sensitive data will be sufficiently trained by the Contractor and informed of any and all obligations and responsibilities with regard to the (potential) consultation of personal data. The Principal may additionally require that a training course as made available by the Principal is followed.
1. **Storing personal data outside UZ Leuven**

For processing whereby personal data leaves UZ Leuven and is stored by the Contractor (or its Sub-processor), the following obligations - in addition to those above - will also apply cumulatively:

* 1. In submitting a tender, the Contractor declares that it is in possession of the following documents. The Contractor will provide the Principal with these at the latter’s request.
		1. The implemented Information Security Policy (ISP) along with a confirmation that the policy has been approved at the highest levels and by various responsible individuals.

The ISP will describe at a minimum:

* + - * how confidentiality, integrity and security will be ensured on input and output, in transit and at rest;
			* what approach to data encryption (including encoding and pseudonymisation) is taken, whether this is applied as a standard on the Contractor's side and who is responsible for this with the Contractor;
			* how the responsibilities and the organisational rules in force are distributed internally;
			* the Security Information and Event Management Plan that analyses security incidents and data logs; and
			* where legally required, the contact details of the information security consultant and/or DPO.
		1. The implemented Back-up and Disaster Recovery Plan that specifies at a minimum:
			- which backup mechanisms are used and whether these are sufficient;
			- which recovery tests are used and whether the reporting on this is available.
		2. The implemented Identity and Access Management (IAM) policy that supports at least the following principles:
			- clearly defined, role-based access rights;
			- withdrawal of access when collaboration ends;
			- strong Authentication;
			- full logging of IAM and data access.
		3. The implemented Incident Management Procedure. This describes at a minimum how the consequences of incidents will be limited for the Principal's data, what steps are to be taken upon the discovery of a security incident and which people are responsible for dealing with the incident to restore the situation to normal.
	1. The Contractor confirms that it fulfils the following technical and organisational requirements:
		1. The data obtained from or via the Principal will not leave the borders of the European Economic Area. Should it leave these borders, the Contractor must supply the necessary guarantees to prove that the transfer meets Chapter V of the General Data Protection Regulation (Transfer of personal data to third countries or international organisations).
		2. The networks over which this data is sent (wired or wireless, from, to or between applications, or via a platform managed by the Contractor, including but not limited to LAN Services, Wide Area Network Services, data centre interconnectivity services, load balancing, SAN switch interconnects and services supplied over Voice over Internet Protocol (VoIP)) have been secured in accordance with the defence-in-depth principle and appropriate techniques are used for the transmission of sensitive data.
		3. The hardware (including VMs) has been equipped with sufficient monitoring and security systems to prevent and analyse data breaches.
		4. The information systems used have been placed in identified and protected premises to which access is limited.
		5. All server systems have been equipped with prevention and detection mechanisms, as well as a means of containing viruses and other malware, and all server systems should have undergone a hardening process.
		6. All server systems have been equipped with a patch management process (implemented and documented).
		7. All patches for server systems are tested in an acceptance environment prior to roll-out.
		8. The systems are subjected to a penetration test and/or ethical hacking at least once a year, preferably in collaboration with the Principal.
	2. The Contractor guarantees its ability to demonstrate the implementation of these measures through external reporting, drawn up once every 3 years at a minimum and in accordance with a carefully described format. On submitting the tender, the Contractor will include the latest external reporting or a document that indicates when, by whom and on what basis the reporting is drawn up.
	3. The Contractor may never decide to alter the Principal's personal data - be it in a manual or automated manner - save for those cases for which explicit permission has been given by the Principal.
	4. The Contractor guarantees that, at the Principal's own choice and request, on (no matter which) termination or expiry of the Basic Agreement or after the expiry of the storage period, all data will be securely destroyed, including all media used for data storage.
1. **Use of Cloud Storage Services for the storage of data outside UZ Leuven**

Where Cloud Storage Services are used, the Principal requires, in addition to the above-mentioned measures, that the Contractor meets the following cumulative conditions:

* 1. A private cloud solution is used or, in a multi-tenant system, the Principal's data is segregated or isolated at a technical level.
	2. The Contractor can ensure the reversibility of the storage system and that of the Sub-processors.
	3. The operation and management of the storage systems is governed by SLAs (Service Level Agreements).
	4. The Contractor can present a business continuity plan at the Principal's request.
	5. The Contractor specifies in its Backup and Retention Plan what Recovery Time Objective and Recovery Point Objective can be met by the Cloud Service.

1. confidential / registered / printed matter

2. title first name last name

3. title and/or department

4. firm or organisation

5. street and number or PO box number

6. postcode and municipality

7. country

**Annex 3**

**Obligations in the context of confidentiality**

In the course of their presence within UZ Leuven, the Contractor and those appointed by it shall abide fully by all regulations and requirements applicable at UZ Leuven, especially those relating to health, safety and hygiene.

They undertake, both during their work at UZ Leuven and afterwards, to treat as confidential any and all information of which they have come to be aware that is or may be of a confidential nature and is directly or indirectly related to the activities of or at UZ Leuven (such as any information on patients, data relating to members of staff or their affairs, reports, corporate information in the broadest sense, information of a medical, technical, financial or commercial nature, etc.).

This also covers all confidential information that is shared by or related to persons or institutions with which they came into contact during their presence at UZ Leuven in any way.

Where, in the context of the assignment, access is provided to UZ Leuven's electronic systems, in particular the KWS (Clinical Workstation), the Contractor or its appointees shall abide fully by all regulations, requirements and procedures applicable to the use of these systems within UZ Leuven.

These include (amongst others):

* Solely one's personal login details to access the system may be used, as assigned by UZ Leuven;
* The personal password must be kept in strictest secrecy;
* Consultation of and any amendments to data, including patient data, is only permitted in the context of the corresponding assignment;
* The Contractor is responsible and liable for all activities carried out under the logins of its appointees;
* The Contractor is responsible for informing its appointees that UZ Leuven keeps logs of all actions taken by the former's appointees.

**Annex 4**

**Sample form for reporting data breaches**

|  |
| --- |
| Details of Principal's contact (reachable 24/7): |
| Service: DPO  |
| Telephone number: 016 33 22 11 – e-mail: gdpr@uzleuven.be  |

|  |
| --- |
| Date: |
|  |
| Company name: |
| Address: |
| Postcode: |
| VAT number: |
|  |
| Who identified the breach? |
| Name: |
| Job Title: |
|  |
| When was the breach identified? |
| Date: |
| Time: |
|  |
| Describe the security incident that led to the breach of personal data security: |
| When did the breach occur? |
| 1. On (date + time)
 |
| 1. Between (date + time) and (date + time)
 |
| 1. Not yet determined
 |
| 1. The incident was reported by an anonymous third party
 |
|  |
| Establish context of the data involved in the breach:  |
| Classification of the data: |
| 1. None, the data cannot be traced back to an individual
 |
| 1. Name and address information
 |
| 1. Telephone numbers
 |
| 1. E-mail addresses, Facebook IDs, Twitter IDs, etc.
 |
| 1. Usernames, passwords or other login details, customer numbers
 |
| 1. Financial information: account numbers, credit card numbers
 |
| 1. National registration number
 |
| 1. Copies of proofs of identity
 |
| 1. Gender, date of birth and/or age
 |
| 1. Data concerning someone's religious or personal beliefs, race, political views or trade unions membership
 |
| 1. Data concerning someone's health or sexual orientation
 |
| 1. Personal data relating to criminal justice or unlawful or disturbing behaviour in respect of an injunction arising from that behaviour
 |
| 1. Data concerning someone's financial or economic situation, information on debts, salary or payment details
 |
| 1. Derived financial data (income category, home ownership, car ownership)
 |
| 1. Lifestyle characteristics (including family composition, living situation, interests), demographic characteristics (age, gender, nationality, occupation, education)
 |
| 1. Data obtained from (public) social media profiles (Facebook, LinkedIn and Twitter accounts, etc.)
 |
| 1. Other, namely:
 |
|  |
| Classification of the context involved in the breach: |
| How many people's personal data are involved in the breach? |
| 1. None, the data cannot be traced back to an individual
 |
| 1. Not yet determined
 |
| 1. At least …………………………………… (number), but not more than ………………………….. (number) involved
 |
| Describe the group of people whose personal data was involved in the breach: |
|  |
| Circumstances of the data breach: |
| 1. Only reading (an unauthorised third party was able to gain sight of (confidential) data. Data is still in possession of the Processor.) - Confidentiality is at risk
 |
| 1. Copying (an unauthorised third party was able to copy data. Again, data is still in possession of the Processor.) - Confidentiality is at risk
 |
| 1. Altering (an unauthorised third party altered data, or was in a position to, in the Processor's system) - Integrity is at risk
 |
| 1. Removal or destruction (an unauthorised third party has removed data from the Processor's system or destroyed it.) - Availability is at risk
 |
| 1. Theft - Availability is at risk
 |
| 1. Not yet known
 |
|  |
| Has the personal data been rendered incomprehensible or inaccessible for unauthorised third parties, for example through encryption or hashing? |
| Yes |
| No |
| Partly, namely |
|  |
| If so, in what manner has the personal data been encrypted: |
|  |
| Does the breach concern individuals from other EU countries? |
| Yes |
| No |
| If so, which EU countries: |
|  |
| What security measures (technical and organisational) have been taken to deal with the breach and to prevent re-occurrence? |
|  |
| Who can be approached for more information on the breach? |
| Name of Contractor's contact: |
| E-mail: |
| Telephone number: |

**Annex 5**

**Sample form for changes to Annex 1 after the processing agreement is concluded**

Where the Parties wish to address certain aspects differently or more specifically, or wish to add certain matters after the processing agreement has been concluded, these should be explicitly agreed with the Principal by means of this form.

**The amendments in this Annex are only valid and enforceable once this Annex has been signed and dated by both parties.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Article** | **Text to be (potentially) removed** | **Replacement or additional text** | **Reason**  |
|   |  |  |  |
|   |  |  |  |
|  |  |  |  |

Agreed and signed in duplicate in ………………………………………….. on …………………………………….. .

**The Principal** **The Contractor**