

# SERVICE PROVIDER AGREEMENT

PROTECTION OF PERSONAL DATA &  
SECURITY OF INFORMATION SYSTEMS

**Version: v.3**



*This document is the exclusive property of the Gustave Roussy Institute. The information it contains may not be reproduced in whole or in part or distributed outside Gustave Roussy without the prior written consent of the Gustave Roussy Institute.*

## ARTICLE 01 - SCOPE

This agreement defines the conditions under which the company, whose registered office is located at, registered in the Trade and Companies Register under the number SIREN : (hereinafter, the "Service Provider), undertakes to carry out, as processor, on behalf of the Gustave Roussy Institute, French non-for-profit research and educational institution, whose registered office is located at 39bis rue Camille Desmoulins, 94805 Villejuif-France (hereinafter, GUSTAVE ROUSSY), as processor for operations concerning the data processing defined in article 3 of this agreement.

## ARTICLE 02 - DEFINITIONS

For the purposes of this agreement, the following words shall be understood :

- "personal data", "data processing", "controller", "processor", "consent" and "violation of personal data" under the terms of the definitions of articles 4 and the following of the Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the data processing and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter the Regulation (EU) N° 2016/679.
- The term "IS" refers to the Information Systems of GUSTAVE ROUSSY;
- The term "Support" refers to GUSTAVE ROUSSY's IT Support in charge of operating GUSTAVE ROUSSY's Information Systems;
- The term "IS Contact" refers to the GUSTAVE ROUSSY staff in charge of monitoring and controlling the service provided by the Service Provider.

## ARTICLE 03 - DESCRIPTION OF DATA PROCESSING

In accordance with the contract(s) or estimate(s) drawn up with GUSTAVE ROUSSY bearing the following number(s) :  
the Service Provider is responsible for :

(hereinafter, the "Service").

To perform the Service, the only personal data processing operations carried out by the Service Provider and any processors are as follows:

collection	extraction	hosting	consultation
cross referencing	modification/manipulation	exchange/sharing	
erasure/destruction			

To perform the Service, the Service Provider may have access to the personal data of the following categories of persons:

patients of GUSTAVE ROUSSY,	donors of GUSTAVE ROUSSY,
GUSTAVE ROUSSY's customers,	GUSTAVE ROUSSY's staff <sup>1</sup> .

The categories of personal data (hereinafter, the "Data") processed by the Service Provider and/or its possible processors, in the context of the Service, concern in particular :

## ARTICLE 04 - COMMON OBLIGATIONS

In accordance with the provisions of Regulation (EU) N° 2016/679 and French Law N° 78-17 of 6 January 1978 on data processing, files and freedom, GUSTAVE ROUSSY and the Service Provider (hereinafter collectively referred to as the "Parties") undertake to take all necessary precautions to ensure that the rights of persons concerned by the Data processing are respected and to preserve, in all circumstances, its security and confidentiality.

## ARTICLE 05 - GUSTAVE ROUSSY OBLIGATIONS

As controller, GUSTAVE ROUSSY undertakes to:

1. Make the Data available to the Service Provider as per the terms and conditions set out in the contract, agreement or convention governing the Service;
2. Specify to the Service Provider the nature and description of the intervention to be carried out, the one-off or repetitive nature of the intervention, the duration of the intervention authorization, the date and the maximum duration of the intervention;
3. If applicable, inform the Service Provider of any limitations or exclusions in connection with the Service;
4. Supervise the Data processing, including audits and inspections, if any, on the Service Provider's premises.

---

<sup>1</sup> *By Gustave Roussy's staff, we mean Gustave's employees, as well as the staff of other legal entities made available to Gustave Roussy (INSERM, CNRS staff, etc.).*

# ARTICLE 06 - GENERAL OBLIGATIONS OF SERVICE PROVIDER

## 06.1 - Data Protection

In the context of the Service, the Service Provider agrees to comply with all the following measures and to ensure that they are respected by its staff and any other person(s) providing their assistance:

1. Consider, with regard to its tools, products, applications or services, the principles of data protection by default, from collection to their complete and irreversible deletion;
2. Process the Data only for the sole purpose of the Service;
3. Take all steps to avoid any accidental or unlawful destruction, accidental loss, alteration or misuse or fraudulent use of the Data;
4. Guarantee the absolute confidentiality of the Data, in particular by not disclosing it to other persons, private or public, natural or legal, except to any processors referred to in this agreement;
5. Not to make any copy of the Data other than necessary for the performance of the Service, without the prior written consent of GUSTAVE ROUSSY;
6. When GUSTAVE ROUSSY so requests, provide it with tools and methods for secure Data exchange between the Service Provider, its possible processors and GUSTAVE ROUSSY;
7. Ensure that the persons authorized to process the Data:
  - a) Agree to respect the confidentiality of the Data or be subject to an appropriate obligation of confidentiality;
  - b) Are given the necessary training in the protection of the personal data;
8. In accordance with the procedures specified in article 18 of this agreement, inform GUSTAVE ROUSSY if it considers that an instruction given by GUSTAVE ROUSSY is a violation of Regulation (EU) N° 2016/679, French Law N° 78-17 of 6 January 1978, its implementing texts, the recommendations of the french national data protection authority (Commission on Information Technology and Freedoms), any other provision of European Union law or the law of the Member States relating to the protection of personal data;
9. In accordance with the procedures specified in Article 18 of this agreement, within a **maximum period of five (5) working days**, report to GUSTAVE ROUSSY any request for access or communication from a third party, whether or not it is backed by an authorization resulting from the application of legal or regulatory provisions in force;
10. Not to transfer the Data outside the territory of the European Union and the European Economic Area (EEA), except in strict compliance with the conditions laid down in Regulation (EU) N° 2016/679, to third countries offering an adequate level of protection within the meaning of Articles 44 to 47 of Regulation (EU) N° 2016-679 to a processor previously authorized by GUSTAVE ROUSSY and signatory to the standard contractual clauses issued by the european authorities.

Where the Service Provider hosts or has a processor host personal data relating to the health of the categories of persons referred to in article 3 of this agreement, the Service Provider, or its possible processor, must first be approved or certified as a Health Data Host (HDH) as per with the provisions L. 1111-8, R. 1111-8-8 and following of the french public health code.

## 06.2 - Security measures

The Service Provider undertakes to define and implement a security policy for its information systems and practices to adapt its operations and activities to the requirements of the regulations covering the protection of personal data.

When the Data is made available to the Service Provider or to one or more of the Service Provider's processors, the Service Provider and, where applicable, its processor(s), undertake to:

- 1) Comply with the notices and recommendations of the Commission on Information Technology and Freedoms, in particular those concerning the security and management rules applicable, especially to archived data, as well as all the security measures defined in the various guides relating to the security of personal data published by the Commission on Information Technology and Freedoms, each in their latest version in force;
- 2) To implement all technical, legal and organizational measures necessary to ensure an appropriate data security level, including in particular the measures referred to in Article 32 of Regulation (EU) N° 2016-679, such as encryption of the Data and their workstations. The implementation of these measures must in particular make it possible to:
  - a) Ensure the confidentiality, integrity and availability of the information systems used to process the Data;
  - b) Take all steps to avoid any accidental or unlawful destruction, accidental loss, alteration or misuse or fraudulent use of the Data;
  - c) Ensure the nominative traceability of persons having access to the Data acting on behalf of the Service Provider and/or its processor(s);
  - d) Ensure full traceability of any incidents related to the Data;
  - e) Regularly test, analyse and evaluate the effectiveness of the technical and organizational measures implemented as part of the Service to ensure data security;
  - f) Restore the availability of and access to the Data within an appropriate time, or, under the terms of the contract drawn up with GUSTAVE ROUSSY where applicable, in the event of a physical or technical incident involving the Service Provider's and/or its processor's information systems;
  - g) To proceed with the destruction of all files, as well as any residual data they may contain relating to the Data, at the end of the Service.

These measures are assessed and corrected by the Service Provider and, where applicable, its processor(s), depending on any incidents that may have occurred in connection with the Service.

At GUSTAVE ROUSSY's request, the Service Provider shall provide it with, as per the procedures specified in article 18 of this agreement, within a **maximum period of ten (10) working days**, the necessary documentation to prove compliance with all the obligations specified above.

## ARTICLE 07 - OBLIGATIONS OF SERVICE PROVIDER FOR ACCESS TO INFORMATION SYSTEMS<sup>2</sup>

When the Service Provider intervenes on the IS, whether on GUSTAVE ROUSSY's premises or remotely, it undertakes in all circumstances to:

- 1) Plan its intervention by informing GUSTAVE ROUSSY in advance as per with the procedures set out in Appendix 1 of this agreement;
- 2) Set up the appropriate human, organizational and technical resources to guarantee IS security;
- 3) Respect the processes defined by GUSTAVE ROUSSY for the proper execution of the intervention;
- 4) Guarantee the nominative traceability of the persons working on its behalf on Gustave Roussy's IS;
- 5) Not damage or exceed the security of the IS and access controls implemented at GUSTAVE ROUSSY;
- 6) Not disrupt the proper functioning of the GUSTAVE ROUSSY IS;
- 7) Connect only to the resources specified in the service request and with one or several accounts suitable for the service;
- 8) Restrict physical and logical access to persons authorized to perform the intervention as part of the service;
- 9) Anticipate the actions necessary for the return to service of the equipment or IS solutions modified as part of the service, such as prior data backup and verification of the proper functioning of the systems concerned by the service;
- 10) Inform GUSTAVE ROUSSY immediately in the event of a risk, suspicion or proven malfunctioning of the IS in accordance with the procedures specified in article 18 of this agreement;
- 11) Send GUSTAVE ROUSSY a report at the end of each service intervention, in accordance with the procedures set out in appendix 2 of this agreement, within a **maximum of five (5) working days after the last day of the service intervention**.

In the event of access to GUSTAVE ROUSSY's premises, the Service Provider shall be accompanied by one or more persons previously designated by GUSTAVE ROUSSY following the request for assistance.

In the event of remote access to the IS, the Service Provider shall send GUSTAVE ROUSSY an updated list of names of the persons who may carry out a remote service intervention as per the procedures specified in article 18 of this agreement.

## ARTICLE 08 – INFORMATION SYSTEMS RESOURCES

If necessary, to enable the Service Provider carry out its service, GUSTAVE ROUSSY shall provide it with the following IS resources:

- One or more nominative accounts for access to the IS according to the need defined within the framework of the Service;
- One or more secure remote access(es) of the *Secure Sockets Layer Virtual Private Network* type.

Any other computer means used to carry out the Service shall be decided jointly by the Parties during the Service.

---

<sup>2</sup> *This article is only enforceable against the Service Provider when the latter intervenes on Gustave Roussy's IS.*

## ARTICLE 09 - SUBCONTRACTING

*(Only 1 checkbox - Indicate the complete list of processors if applicable)*

Option A : On the date of signature of this agreement, the Service Provider is authorized to call upon :

Option B : On the date of signature of this agreement, the Service Provider does not subcontract any data processing in connection with the Service.

Throughout the duration of the Service, the Service Provider may use other processors to carry out specific data processing activities. In this case, the Service Provider shall inform GUSTAVE ROUSSY, in accordance with the procedures specified in article 18 of this agreement, of any proposed change concerning the addition or replacement of other processors. This information shall clearly indicate the outsourced data processing activities, the identity and contact details of the processor (including the country where he is located) and the predicted dates of the subcontracting agreement.

GUSTAVE ROUSSY has a **maximum period of fifteen (15) working days** from the date of receipt of this information to make any objections. This subcontracting may only be carried out if GUSTAVE ROUSSY has not raised an objection within the agreed period.

All the Service Provider's processors are required to comply with the obligations of this agreement on behalf of and in accordance with the instructions of GUSTAVE ROUSSY.

It is the Service Provider's responsibility to ensure that its processors comply with all the obligations to which it is itself subject under the terms of this agreement.

## ARTICLE 10 - EXERCISE OF THE RIGHTS OF THE PERSONS CONCERNED

It is the responsibility of GUSTAVE ROUSSY to respond to requests for the exercise of the rights of persons concerned by the Data processing.

When these persons exercise their rights directly with the Service Provider, the latter shall forward their requests to GUSTAVE ROUSSY within a **maximum of six (6) working days** in accordance with the procedures specified in article 18 of this agreement.

When the examination of these requests requires the support of the Service Provider, the latter shall have a **maximum of twelve (12) working days** to carry out the operations necessary to examine these requests, on receipt of GUSTAVE ROUSSY's written request for support.

## ARTICLE 11 - NOTIFICATION OF DATA BREACH

As soon as it becomes aware of it and within a **maximum of two (2) calendar days**, the Service Provider shall notify GUSTAVE ROUSSY of any breach of the Data in accordance with the terms and conditions specified in article 18 of this agreement.

The Service Provider shall provide GUSTAVE ROUSSY with the following information relating to the breach of the Data at the time of notification of the incident, or if this is not reasonably possible as soon as possible after notification of the breach:

- 1) The nature of the Data breach ;
- 2) The estimated number of people involved ;
- 3) The categories of the person(s) involved ;
- 4) The categories of Data concerned ;
- 5) The estimated number of Data that have been violated ;
- 6) The measures that have been taken to remedy the Data breach, including, where applicable, measures to limit adverse effects and potential risks.

The Service Provider shall assist GUSTAVE ROUSSY as far as possible in reporting the breach of the Data to the competent control authority and/or to the person(s) involved in the Data breach.

## ARTICLE 12 - DATA OUTCOME<sup>3</sup>

*(only 1 checkbox)*

At the end of the Service, the Service Provider undertakes, after having ascertained the terms and conditions relating to reversibility :

To destroy all Data

To return all Data to GUSTAVE ROUSSY

To return the Data to the processor designated by GUSTAVE ROUSSY

In the event of the Data being returned, the return must be accompanied by the destruction of all of the Data (including copies) in the information systems of the Service Provider and any processors.

In any event, the Service Provider, as well as its processors, shall irreversibly destroy all the Data (including copies) within a **maximum of fifteen (15) working days at the end of the Service**, or following the return of the Data, unless the preservation of such data is required pursuant to article 28 of Regulation (EU) N° 2016/679. In this case, the Service Provider shall inform GUSTAVE ROUSSY, in accordance with the procedures specified in article 18 of this agreement, of any proposed change concerning the addition or replacement of other processors.

Once the Data has been destroyed (including copies), the Service Provider shall issue a certificate of destruction and submit it to GUSTAVE ROUSSY, as per the procedures specified in article 18 of this agreement, within a **maximum of five (5) working days**.

This certificate contains precise information on the destruction process, a table containing the list of files, the date of destruction, and the signature of the official agent authorized by the Service Provider.

---

<sup>3</sup> *This article is not enforceable against the Service Provider when the latter only has access to the Data for the purpose of consultation on the strict condition that he does not make any copies of the Data under the terms of the Service.*



## ARTICLE 13 - REFERENTS

On the day this agreement is signed:

- The persons acting as Data Protection Officer are:
  - For the Service Provider :
  - For GUSTAVE ROUSSY : Emmanuel PLANCHET : [donneespersonnelles@gustaveroussy.fr](mailto:donneespersonnelles@gustaveroussy.fr).
- The persons acting as Chief Information Security Officer are:
  - For the Service Provider :
  - For GUSTAVE ROUSSY : Cédric LEMOINE: [donneespersonnelles@gustaveroussy.fr](mailto:donneespersonnelles@gustaveroussy.fr).

## ARTICLE 14 – RECORD OF PROCESSING ACTIVITES

The Service Provider declares that it keeps a written record listing the data processing carried out on behalf of GUSTAVE ROUSSY.

## ARTICLE 15 - DOCUMENTATION

When GUSTAVE ROUSSY so requests, the Service Provider shall provide it with the necessary documentation to demonstrate compliance with all its obligations, which may in particular enable audits, including inspections, to be carried out by GUSTAVE ROUSSY or another auditor it has appointed, and shall contribute to such audits.

This documentation shall be communicated to GUSTAVE ROUSSY in accordance with the procedures specified in article 18 of this agreement within a **maximum of ten (10) working days**.

This documentation is produced and communicated at the Service Provider's expense.

## ARTICLE 16 - AUDIT

Before the start of the Service and at regular intervals, within the limit of one audit per calendar year, GUSTAVE ROUSSY may carry out an audit to verify the Service Provider's compliance with its commitments under this agreement.

GUSTAVE ROUSSY shall inform the Service Provider of any audit decision at **least fifteen (15) working days** before the start of the audit. The information provided to the Service Provider specifies the purpose of the assignment, the date and duration of the audit and the identity and references of the persons in charge of the audit.

The persons in charge of the audit may not be direct competitors of the Service Provider and are subject to a strict obligation of confidentiality.

The Service Provider shall set up reasonable means to enable the persons in charge of the audit to carry out their mission. The audit may only be carried out during the Service Provider's business hours and shall not cause the undue disruption of its activities. In the event of a significant disruption of its activities, the Service Provider reserves the right to suspend the audit and to notify GUSTAVE ROUSSY accordingly.

If GUSTAVE ROUSSY identifies a need for an additional audit during the same calendar year, a request to this effect shall be submitted in writing to the Service Provider. The Service Provider may refuse this new audit unless the audit request is made following a notification of a Data breach.

Audits are carried out at the expense of GUSTAVE ROUSSY.

## ARTICLE 17 – DATA PROTECTION IMPACT ASSESSMENT

If GUSTAVE ROUSSY so requests, the Service Provider shall assist it with a data protection impact assessment within **sixteen (16) working days**, as per the terms of the procedures specified in article 18 of this agreement.

This data protection impact assessment is carried out at Gustave Roussy's expense.

## ARTICLE 18 - INFORMATION AND ALERTS SENT TO GUSTAVE ROUSSY

The information and alerts sent to GUSTAVE ROUSSY referred to in articles 6.1, 6.2, 7, 9, 10, 10, 11, 12, 15 and 17 will be sent by e-mail to the following addresses: [donneespersonnelles@gustaveroussy.fr](mailto:donneespersonnelles@gustaveroussy.fr) and [intervention.prestataire@gustaveroussy.fr](mailto:intervention.prestataire@gustaveroussy.fr).

## ARTICLE 19 - LIABILITY AND INSURANCE

Each Party is liable to the other Party and third parties for its obligations under this agreement and/or the regulations in force regarding the protection of personal data, whether the data processing is performed by itself, its employees and/or its processors.

Each Party shall be liable for any direct and/or indirect damages caused by its own fault, that of its employees and/or processors, in the event of failure, fault and/or negligence under the conditions of ordinary law and shall compensate the injured Party, notwithstanding the liabilities provided for in the service agreement described in article 3 with which this agreement is associated.

The Service Provider shall take out and maintain in force the necessary insurance to cover its liability.

## ARTICLE 20 - TERMINATION

In the event of non-performance and/or failure by the Service Provider and/or its processor(s) to comply with articles 6.1, 6.2<sup>4</sup>, 7<sup>5</sup>, 8<sup>6</sup>, 9, 11, 15, 16, 17 and 18 of this agreement, GUSTAVE ROUSSY reserves the right to terminate the Service drawn up with the Service Provider described in article 3 of this agreement after a **period of one (1) month** following formal notice. The termination of the Service contracted with Gustave Roussy shall not allow any recourse or damage claim by the Service Provider and to the payment of any compensation.

This formal notice shall be sent to the Service Provider by GUSTAVE ROUSSY by registered letter with acknowledgement of receipt. The **one (1) month deadline** shall begin to run from the date of receipt of this letter by the Service Provider.

At the end of the Service, or in the event of early termination, the Service Provider shall return to GUSTAVE ROUSSY, immediately under the penalty of incurring liability, all the elements and the documents produced by the Service Provider in the performance of the service(s).

---

<sup>4</sup> *If applicable to this service*

<sup>5</sup> *If applicable to this service*

<sup>6</sup> *If applicable to this service*

The early termination of the contract(s), agreement(s) or service convention(s) signed by the Service Provider and GUSTAVE ROUSSY shall not exempt the Service Provider from fulfilling its obligations with GUSTAVE ROUSSY until the effective termination date, subject to any damage suffered by GUSTAVE ROUSSY as a result of the early termination of the service(s).

Early termination of the contract(s), agreement(s) or service convention(s) shall not exempt the Service Provider from deleting or returning the Data under the terms and conditions set out in article 12 of this agreement

## ARTICLE 21 - LEGAL VALUE

It is expressly understood between the Parties that the clauses of this agreement shall override any other contractual clauses relating to the protection of personal data in respect of the Service provided by the Service Provider and its possible processor(s).

## ARTICLE 22 - APPLICABLE LAW AND EFFECTIVE DATE

French law is applicable to this agreement.

This agreement shall take effect on the date of signature.

By signing this agreement, the Parties acknowledge that they have read it in its entirety and undertake to apply all of its provisions.

Signed on :

At:

Submitted in two (2) original copies to the Parties, each retaining one (1) original copy.

### SIGNATURE OF SERVICE PROVIDER

### SIGNATURE OF GUSTAVE ROUSSY

*NB: Each of the signatories acknowledges that they are duly authorized by their company to sign this agreement.*

This agreement is free of any handwritten annotation except for the date and place of signature and the signature of the Service Provider. Any other handwritten annotation will render this agreement null and void.

## APPENDIX 1 - ACCESS TO THE IS: REPORT IN CASE OF INTERVENTION

When the Service Provider accesses GUSTAVE ROUSSY's IS, it informs the requesting party and the IT referent (of GUSTAVE ROUSSY's Digital Conversion and Information Systems Department - hereinafter, the "DTNSI"), if the latter is identified. The Service Provider ensures that the following e-mail address is a copy of the exchanges: [intervention.prestataire@gustaveroussy.fr](mailto:intervention.prestataire@gustaveroussy.fr).

The request for action shall indicate at least :

1. The reason for the intervention ;
2. The identity of the intervener(s) ;
3. The scope of the intervention ;
4. The equipment or resources concerned by this intervention ;
5. The desired date and duration of the intervention ;
6. The expected impact on the IS and/or Data ;
7. If applicable, the identity of the requesting party for GUSTAVE ROUSSY ;
8. If applicable, the expected unavailability period of the IS and/or Data ;
9. If applicable, the type of competence of GUSTAVE ROUSSY required to support the intervention.

## APPENDIX 2 - ACCESS TO INFORMATION SYSTEMS - INTERVENTION REPORT

The Service Provider's report is submitted to the GUSTAVE ROUSSY DTNSI Department by e-mail, to the requesting party, and to the IT referent, if the latter is identified, and to the following e-mail address: [intervention.prestataire@gustaveroussy.fr](mailto:intervention.prestataire@gustaveroussy.fr).

This intervention report is communicated to GUSTAVE ROUSSY five (5) working days maximum after the last day of intervention.

This report shall contain at least the following information :

1. A reminder of the request for action ;
2. An explanation of the service(s) performed ;
3. A list of the persons involved during the intervention on behalf of the Service Provider ;
4. A description of the Data collected and deleted ;
5. The scope of the intervention ;
6. If applicable, the duration of material and/or service unavailability ;
7. Recommendations or actions still to be carried out.