

REGISTER OF PROCESSING IMPLEMENTED BY GUSTAVE ROUSSY / Privacy Impact Assessment

Activity 6 – Health Research

Project Name / Processing	AFTER T DXD
Responsible for the processing of personal data	Gustave Roussy
Coordinates	39 bis rue Camille Desmoulins, 94800, Villejuif
Contact details of the Data Protection Officer (DPO)	Mrs. Clara Bechet clara.bechet@gustaveroussy.fr
Purposes of the processing:	
Purpose 1	Patterns of Treatment after progression of Disease to Trastuzumab Deruxtecán (T-Dxd) a HER2-positive metastatic breast cancer.
Purpose 2	
Purpose 3	
Legal basis for processing	The processing is based on two complementary legal bases: the legal basis for data processing provided for in Article 6 of the GDPR and the specific legal basis of Article 9 of the GDPR applicable to sensitive data (health data). Within the meaning of <u>Article 6.1 of the GDPR</u> , data processing is based on the performance of a mission in the public interest or within the public authority vested in Gustave Roussy, as a Cancer Center contributing to the missions of the public research service, to conduct research in the field of health in order to better understand them, curing and preventing them (Article 6.1.e). Within the meaning of <u>Article 9.2 of the GDPR</u> , the legal basis is that of carrying out the processing of data for the purposes of scientific research (Article 9.2.f).
In-house or multi-center research	Multicentric
Multicentric IS: List of data providers (e.g., partner centers)	<ul style="list-style-type: none"> - Centre François Baclesse - Limoges University Hospital - Centre Léon Bérard - Centre Eugène Marquis - Centre Antoine Lacassagne - Regional Cancer Institute of Montpellier - Oncopole de Toulouse - Gustave Roussy Cancer Center - Istituto Europeo di Oncologia - Azienda Ospedaliera Ordine Mauriziano, Torino - Azienda Ospedaliera Careggi, Firenze - Humanitas, Catania - Istituto Nazionale Tumori Pascale Napoli
Multicentric IS: Data recipients / external partners (e.g. processors)	No outgoing transfer
Research Category	<input type="checkbox"/> Clinical Drug Trial

	<input type="checkbox"/> RIPH1 <input type="checkbox"/> RIPH 2 <input type="checkbox"/> RIPH 3 <input checked="" type="checkbox"/> Non-RIPH (retrospective study) <input type="checkbox"/> Medical Device Clinical Investigation (MD) <input type="checkbox"/> In Vitro Diagnostic Medical Device (IVDM) Performance Study
Compliance with a standard (MR001, MR0002, MR003, MR004 etc.)	MR-004 French Data Protection Authority compliance (see checklist)
Categories of data subjects	<input checked="" type="checkbox"/> Patients <input type="checkbox"/> Healthcare professionals
Categories of data processed	
Persons Suitable for Research	
General identification data	<input checked="" type="checkbox"/> Age <input type="checkbox"/> Place of Birth <input type="checkbox"/> Gender <input type="checkbox"/> Country and department of residence <input checked="" type="checkbox"/> Patient ID <input type="checkbox"/> Ethnicity Justification: Pseudonymization
Social Security Number (NIR) or equivalent	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Health data	<ul style="list-style-type: none"> - Vital status - Date of diagnosis - Biological data - Pathological features of the primary tumor - Date of recurrence and its pathological characteristics - Treatments received after T-DXd - Response and duration of treatment - Current Treatment - Reason for discontinuation of treatment - Date of last follow-up - Date of death Genetic (or genomic) data: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If applicable: <input type="checkbox"/> Somatic <input type="checkbox"/> Constitutional Justification: This data is necessary to meet the purpose of the study.
Other data	<input type="checkbox"/> Photo/ Video

	<ul style="list-style-type: none"> <input type="checkbox"/> Level of education <input type="checkbox"/> Professional life <input type="checkbox"/> Mutual <input type="checkbox"/> Displacement <input type="checkbox"/> Tobacco/alcohol/drug use <input type="checkbox"/> Lifestyle (urban, rural, etc.) <input type="checkbox"/> Repayment <input type="checkbox"/> Family situation <input type="checkbox"/> Socio-professional category <input type="checkbox"/> Social security scheme <input type="checkbox"/> Lifestyle Habits / Behaviors <input type="checkbox"/> Sex life <p>Rationale : Click here to type text.</p>
Data relating to other persons	<ul style="list-style-type: none"> <input type="checkbox"/> Family history <p>Rationale : Click here to type text.</p>
Research professionals	
Identity data	<ul style="list-style-type: none"> <input type="checkbox"/> Name and/or surname <input type="checkbox"/> Postal contact information <input type="checkbox"/> Email contact information <input type="checkbox"/> Telephone contact information <input type="checkbox"/> Bank details
Business Data	<ul style="list-style-type: none"> <input type="checkbox"/> Diploma Training(s) <input type="checkbox"/> Professional life <i>(including professional background, mode and type of practice, elements necessary to assess the knowledge they have to carry out the research)</i> <input type="checkbox"/> Identification number in the shared directory of healthcare professionals <input type="checkbox"/> Amount of allowances and remuneration received <input type="checkbox"/> Collaboration with other studies <input type="checkbox"/> History of access and connections to the medical data of people participating in a research <p>Rationale : Click here to type text.</p>
Data Origin	
The personal data will be collected indirectly from the data subjects, from their patient file.	

Are the purposes of the processing determined, explicit and legitimate ?	
All the data processed in this context were collected to precisely answer the scientific question posed by the protocol, making this collection de <i>facto</i> relevant and contributing to the legitimacy of the processing. To illustrate, no data was collected "just in case" and the choice of data collected is based on their adequacy with regard to the objectives of the treatment, further away from the study. In addition, the processing of data is explicit in that specific information on the study, comprehensible, and containing the information prescribed by Articles 13 and 14 of the GDPR will be delivered to the data subjects.	
Data minimization measures <i>(Including locations and access to lookup tables)</i>	
The personal data is previously pseudonymized in accordance with Gustave Roussy's data pseudonymization procedure. Thus, the identifier and quasi-identifier attributes have been removed. Also, the day of birth is not collected, for minimization measures but also to comply with the applicable Frenche Data Protection Authority (FDPA / CNIL)'s reference methodology. In addition, a specific inclusion number, other than the patient record number, is generated as part of the study to further minimize data processing. The creation of this number complies with the prerequisites of the FDPA / CNIL's reference methodology applicable to the study: MR-004. Finally, only the data strictly necessary to answer the scientific question of the study will be processed. All these measures contribute to mitigating, or even rendering non-existent, the risks to the rights and liberties of the data subjects.	
Is there a collection of data or samples that are not strictly necessary to achieve the objectives of the research (additional data collected for another use)?	
<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If yes, specify: Click here to type text.	
Infrastructure/information system used <i>(databases, media, operating tools, etc.) and point of contact at the processors or joint controllers (specify roles)</i>	
Source database: computerized patient record / working database: REDCAP software	
Access to data	
Gustave Roussy	<input type="checkbox"/> Access within the care team <input checked="" type="checkbox"/> Access outside the care team If so: is the data pseudonymized or anonymized? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Excluding Gustave Roussy	No data transfer outside of GR, only for data provider centers.
Conservation	
Where	Redcap to Gustave Rousy
Retention period	2 years from the publication of the research results, in the absence of publication, until the signature of the final report, i.e.: 4 years.

Archiving			
Where	NA		
Archiving period	NA		
Data quality			
The personal data come from medical documents written in clinical routine by the medical staff of the institutions participating in the study. The data is not modified, it is extracted and structured within the framework of the study.			
Contractual framework(s)			
A data transfer contract (DTA) has been set up with each of the partner centres and data providers in order to implement the respective obligations of each within the meaning of the GDPR.			
Regulatory framework			
The study has received the favorable opinion of Gustave Roussy's Internal Ethics Committee and complies with the MR-004 of the CNIL.			
Data transfer outside the EU			
<input type="checkbox"/> Suitable country <input type="checkbox"/> Inadequate country If the country is not suitable, specify the additional legal measures: <input type="checkbox"/> Standard Contractual Clauses (SCCs) <input type="checkbox"/> Code of Conduct			
Rights of data subjects	Provided for in the information note / consent form?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Rationale : V. Information note		
Right to introduce a complaint to the CNIL	Provided for in the information note / consent form?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
	Rationale : V. Information note		
Risks			
	Illegitimate access	Unwanted change	Disappearance
<i>Potential impacts</i>	Material, moral	None	None
<i>Sources of risk</i>	Internal/External/Non-Human Sources	Internal/External/Non-Human Sources	Internal/External/Non-Human Sources
<i>Threats</i>	Access given to an unauthorized person internally or from an investigator center or external intrusion (hacker)	Access given to an unauthorized person internally or from an investigator center or external intrusion (hacker)	Access given to an unauthorized person internally or from an investigator center or external intrusion (hacker)

<p><i>Measures to address the risk</i></p>	<p>Data metrics</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Encryption <input type="checkbox"/> Anonymization <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Pseudonymization (e.g., concordance table) <input checked="" type="checkbox"/> Partitioning <input checked="" type="checkbox"/> Logical access control <input checked="" type="checkbox"/> Journaling <input checked="" type="checkbox"/> Archiving (in the common sense) <input checked="" type="checkbox"/> Securing paper documents <input checked="" type="checkbox"/> Data minimization <p>General measurements of the system (specific to Gustave Roussy)</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Securing the operation <input checked="" type="checkbox"/> Fight against malware <input checked="" type="checkbox"/> Workstation Management <input checked="" type="checkbox"/> Website protection <input checked="" type="checkbox"/> Data backup <input checked="" type="checkbox"/> Maintenance <input checked="" type="checkbox"/> Subcontracts <input checked="" type="checkbox"/> Security of IT channels <input checked="" type="checkbox"/> Physical Security <input checked="" type="checkbox"/> Traceability <input checked="" type="checkbox"/> Securing equipment <input checked="" type="checkbox"/> Removal of sources of risk <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Protection from non-human sources of risk <p>Organisational measures (specific to Gustave Roussy)</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Organization of privacy policy <input checked="" type="checkbox"/> Manage the privacy policy <input checked="" type="checkbox"/> Managing Risk <input checked="" type="checkbox"/> Integrating privacy into projects <input checked="" type="checkbox"/> Manage security incidents and data breaches <input checked="" type="checkbox"/> Personnel management <input checked="" type="checkbox"/> Management of third parties accessing data <input checked="" type="checkbox"/> Overseeing privacy
<p><i>General Measures- Personnel Management</i></p>	<p>Gustave Roussy employees with access to the data sign a GDPR Annex to their employment contract when they arrive and read the User Charter detailing the data access policies. In addition, awareness-raising sessions carried out by Gustave Roussy's DPO reminding people of the obligations in terms of personal data protection are carried out frequently. Targeted awareness-raising actions are regularly carried out with the staff concerned on themes specific to their role and the sensitivity of the data they process.</p>
<p><i>General Measures – Overseeing Privacy</i></p>	<p>As Gustave Roussy is required to process sensitive data (health data) on a large scale, Gustave Roussy has a DPO, Mrs. Clara Bechet, who was recruited on October 4, 2021 and appointed to the CNIL. Gustave Roussy's DPO is in charge of advising and supporting Gustave Roussy's community of professionals in the compliance of the data processing carried out with the regulations in force, in particular and not limited to research.</p>

<i>General Measures – Managing Data Protection Incidents</i>	Data protection responsibilities are defined contractually within the framework of the project, through the data transfer contracts put in place. In addition, a data breach management process that allows for rapid response and remediation is also put in place and a specific video about personal data breach was made by the DPO of Gustave Roussy and is regularly transmitted to professionals.		
<i>General Measures – Physical Security</i>	Access control by individual badge to access the Gustave Roussy premises, access control by individual badge restricted to the server room and video protection and video surveillance system. 24/7 presence of security guards.		
<i>Gravity</i>	<input type="checkbox"/> 1 – Negligible <input type="checkbox"/> 2 - Limited <input checked="" type="checkbox"/> 3 - Important <input type="checkbox"/> 4 – Maximum	<input checked="" type="checkbox"/> 1 – Negligible <input type="checkbox"/> 2 - Limited <input type="checkbox"/> 3 - Important <input type="checkbox"/> 4 – Maximum	<input checked="" type="checkbox"/> 1 – Negligible <input type="checkbox"/> 2 - Limited <input type="checkbox"/> 3 - Important <input type="checkbox"/> 4 – Maximum
<i>Likelihood</i>	<input type="checkbox"/> 1 – Negligible <input checked="" type="checkbox"/> 2 - Limited <input type="checkbox"/> 3 - Important <input type="checkbox"/> 4 – Maximum	<input type="checkbox"/> 1 – Negligible <input checked="" type="checkbox"/> 2 - Limited <input type="checkbox"/> 3 - Important <input type="checkbox"/> 4 – Maximum	<input type="checkbox"/> 1 – Negligible <input checked="" type="checkbox"/> 2 - Limited <input type="checkbox"/> 3 - Important <input type="checkbox"/> 4 – Maximum
<i>Feedback</i>	As the study is purely retrospective, no impact on the persons concerned will be characterized in the event of an infringement of the integrity or availability of the data. In the event of a breach of confidentiality, prejudice may arise for the persons concerned (employment discrimination, insurance discrimination), provided that the technical and organisational measures put in place, including the minimisation of data processing, considerably reduce the occurrence and likelihood of the risk.		
Record Writer(s)	Gugliano Federica and DPO of GR		
Last updated date	02/05/2025		
DPO / CISO validation	Validation from DPO		

WHY FILL OUT THIS FORM?!

What is the purpose of this form? This form feeds into a register that lists all the research projects in which Gustave Roussy participates, whether it is a sponsor, investigator, data controller, subcontractor, etc.

Is it mandatory? YES. Gustave Roussy is legally obliged to keep a register of all personal data processing and the registration of your project on this Register is an essential regulatory prerequisite to ensure its proper compliance.

When to fill out this form? Upstream of the implementation of the research, more precisely, before any processing of personal data.

