DATA PROTECTION IMPACT ASSESSMENT

Context

Overview

What is the processing under consideration?

The collection of personal data related to patients and heath care professionals in the context of VINOREAL study (hereafter the "Study").

VINOREAL is a multicenter, multi-country, retrospective and prospective, observational, study to describe the current real-world effectiveness and safety data of OV-based treatments as well as the patient's healthcare pathway and quality of life (QoL) associated with this treatment of patients with Advanced Breast Cancer (ABC) using FACT-B, PPQ, and WPAI questionnaires.

The Study will be conducted in 3 identified countries: Italy, Algeria, and China.

The Study population will consist of:

- Retrospectively enrolled patients, meaning patients aged ⩾ 18 years (⩾ 19 years for Algeria as per local regulation) at OV-based treatment initiation who initiated OV treatment for ABC between 2011 and 2020.
- Prospectively enrolled patients, meaning patients aged ⩾ 18 years (⩾ 19 years for Algeria as per local regulation) at OV-based treatment initiation who initiate OV treatment at or after inclusion in the study and eligible for prospective collection of QoL data and PPQ and WPAI questionnaires.

Given the above, Pierre Fabre Medicament will process personal data relating to:

- Living patients who have given their consent by signing the Informed Consent Form or did not oppose to the processing of personal data, having read the Privacy Information Notice on the processing of personal data carryout out by Pierre Fabre in the context of the study, and,

1. . Deceased patients for whom the Privacy Policy may be made available, and the relevant Informed Consent Form may be signed by a legal representative and for Italy, according to art. 110 of Legislative Decree 196/2003 (hereinafter, the "Privacy Code"), as further amended by art. 44 co 1 bis L. 29/04/2024 n. 56 as better specified in this document.

What are the responsibilities linked to the processing?

1. Pierre Fabre Medicament S.A. (Pierre Fabre), a company with registered office in Les Cauquillous - 81500 Lavaur (France), acts as a sponsor of the Study and as the controller of the personal data of Data Subjects within the framework of Studio Fortrea France S.a.r.l., with registered office at 2 rue Jacque Daguerre, 92500 Rueil-Malmaison (France), acts as a Data Processor duly designated by Pierre Fabre through a Data Processing Agreement pursuant to Article 28 of the GDPR, which as CRO assists Pierre Fabre Medicament in the management of the activities related to the Trial (including, relations with the ethics committees and institutions of the Sites, the collection and transmission of pseudonymised personal data of Patients, the collection and management of data and the final communication of pseudonymised results, etc.), acting as a data processor.

- Fortrea with principal offices located at 2 rue Jacque Daguerre, 92500 Rueil-Malmaison (France) is acting as Data Processor duly designated by Pierre Fabre Medicament through a Data Processing Agreement pursuant to Article 28 of the GDPR, which as a CRO assists Pierre Fabre Medicament in the management of the activities related to the Study (including, relations with ethics committees and institutions in the Sites, collection and transmission of Patients' pseudonymized personal data, the data collection and management and the final reporting of pseudonymized results, etc.), acting as the data processor.

The Sites, including hospitals and medical centers participating in the Study, as well as treating physicians (investigators) experienced in the administration of anti-cancer medications, and prescribing treatments to Patients are acting as Data Controller for the medical files related to the study participants.

- Any third-party providers of the technological infrastructure used by the Sponsor for the performance of the Study which, in any event, do not have access to the processed data.

Are there standards applicable to the processing?

Several European and national standards dealing with both good clinical practices (European GCP) and data privacy regulations are applicable to this processing (GDPR and national regulations related to data protection).

Specificity of Italy:

On April 23, 2024, the Italian Parliament approved an amendment to the Privacy Code relating to Article 110 on "Medical, biomedical and epidemiological research".
More precisely, the obligation for Sponsors to consult in advance the Italian Data Protection Authority (Garante) and obtain its opinion before conducting studies involving the processing of health data for scientific purposes, and when it is impossible to obtain patients' consent, or to inform data subjects is "impossible" or involves "a disproportionate effort" or risks "preventing or seriously damaging the achievement of the objectives of research".

Although this obligation has ceased, PF has put in place appropriate measures to protect the rights, freedoms and legitimate interests of data subjects prior to the processing of personal data:

The Data Protection Impact Assessment will be published on the PF website (https://clinicaltrials.pierre-fabre.com) and communicated to the Authority.
- The study will be reviewed and approved by the competent Ethics Committee in Italy.
- Patients receive the Privacy Policy and express their consent to the processing of personal data by signing the informed consent form
- For deceased patients, the centers make reasonable efforts to obtain consent from their legal representatives by contacting them at the last known address. The center reports it in the patients' medical records.
- For deceased and unreachable patients, as this would involve a disproportionate effort or risk jeopardising the purpose of the Study in accordance with Article 14(5) and recital 62 of the GDPR, a notice will be published on the PF website and on the Centre's website, as well as posted in the Centre's waiting room, when possible, allowing data subjects to have access to the Privacy Policy and exercise their rights.

Context

Data, processes and supporting assets

What are the data processed?

The following key data items will be collected, where available:

- Patient demographic and clinical characteristics at initial diagnosis of ABC or start of OV treatment (both cohorts).
- Treatment history for breast cancer and ABC since diagnosis and before OV treatment initiation (both cohorts).
- OV treatment for advanced breast cancer (both cohorts) from treatment initiation to permanent discontinuation.
- Concomitant anti-cancer treatments: start date, end date, dose, reason for dose change/interruption/discontinuation for each treatment dose administered and each treatment interruption.
- Clinical outcome after OV permanent discontinuation (both cohorts).
- Adverse events (both cohorts).
- Subsequent line(s) of treatment for breast cancer after oral vinorelbine treatment discontinuation (both cohorts).
- Healthcare access and pathway (both cohorts).
- QoL data for prospectively included patients only.
- Patients' preference for route of treatment administration for prospectively included patients only.
- Work productivity for prospectively included patients only.

Who are the data subjects envisaged by the Process and what number of data subjects are expected to be impacted by this Process?

The Process will involve the processing of approximately 368 Patients participating in the Study:

- 130 retrospective patients (including 40 for Italy)
- 238 prospective patients (including 30 for Italy)

Italian sites participating in the Study include the following Sites:

- Site No. 38001 – IRCCS San Gerardo dei Tintori, Phase 1 research center – Approval date 29 February 2024
- Site No. 38003 – Ospedale San Martino di Belluno, UOC Oncologia – Approval date 29 February 2024
- Site No. 38004 – IRCCS Ospedale Policlinico San Martino – Approval date 29 February 2024

In particular, the Study population will consist of:

- Retrospectively Enrolled Patients, meaning Patients who started OV treatment for ABC between 2011 and 2020 will be enrolled in the retrospective cohort study. The observation period for retrospectively included patients will extend from the initiation of OV treatment to the date of death, date of last contact or end date of retrospective observation period, whichever occurs first. The end date of retrospective observation period will be set as the date of the inclusion of the first patient in the study (First Patient In= FPI).
- Prospectively Enrolled Patients, meaning Patients initiating OV treatment and eligible for prospective collection of QoL data and PPQ and WPAI questionnaires will be enrolled in the prospective cohort study. The enrollment period is expected to extend up to 17 months from study start. The study observation period will extend up to 2 years after last patient first visit (around 24 months after treatment initiation).

Given the above, Pierre Fabre will process personal data relating to:
- Living Patients who have given their consent to the processing of personal data by signing the Informed Consent form, having read the Privacy Information Notice on the processing of personal data carried out by Pierre Fabre in the context of the Study for Italy as in Algeria and China, some sites may benefit from waivers; and

- Deceased Patients for whom the Privacy Information Notice can be made available and the related Informed Consent Form can be obtained from a successor in title, legal representative, or anyone acting on behalf of the deceased as his or her representative, or for Italy, on the basis of Article 110 of the Italian Legislative Decree No. 196/2003, as further amended by art 44 co 1 bis l. 29/04/2024 n. 56 (hereinafter, the "Privacy Code") as further explained throughout this document.

In any case, Patients must be ≥ 18 years (≥ 19 years for Algeria as per local regulation) at OV-based treatment initiation to be eligible for the Study.

When patients agree on the participation to the study, the following steps will be carried out:
1) Data collection and data entry by investigators of the sites – To this end, data collected from patients' medical records will be entered by the sites in a separate electronic case report form, namely "electronic Case Report Form" ("eCRF"), for each patient. Prospectively enrolled patients will be given a paper diary at inclusion containing the instructions and schedule for questionnaires completion as well as the batch of blank questionnaires to be completed as per the specific schedule. The site investigator or qualified designee will record the answers in the eCRF.

2) Pseudonymization of data – Sites will upload data into the Electronic Data Capture ("EDC") system that the Sponsor, by means of the CRO, will use to store and analyze data collected. The EDC will retain pseudonymized (key-coded) personal data only in order not to allow the Sponsor (and, thus, the CRO) to directly identify patients. Indeed, only the relevant site will have access to both the patients' ID and the directly identifiable information of each patient. The Sponsor (and the CRO), instead, will not have access to the identifying data of each patient, including name and surname, and will not be able to link each patient ID to the relevant patient, since data entered into the EDC by the sites will be already key-coded, thus pseudonymized.

3) Data analysis process – Data entered into the eCRF will be reviewed for consistency by the competent data manager using both automated logical checks (i.e., issuing in automatic queries generated by the system) and manual review (i.e., issuing in manual checks set by the data manager or the monitor into the eCRF). All data collected within the eCRF will be approved and electronically signed and dated by the investigator or designee. This approval will acknowledge the investigator's review and acceptance of the data as being complete and accurate. At study end and before the final statistical analysis, the e-CRF and other study data will be locked to further additions or corrections. Locking the study data represents the acknowledgement that all data have been captured and confirmed as accurate.

4) Drafting of Study Report – The data analyzed will be documented in a study report and communicated, in an aggregate manner, by Fortrea to Pierre Fabre Medicament. This step will be carried out by Fortrea, on Pierre Fabre Medicament's behalf. Quality assurance representatives from Fortrea or Pierre Fabre Medicament may visit a Site to conduct quality assurance audit and ensure the Study is conducted in compliance with the Protocol, Standard Operating Procedures (SOP) and all applicable law requirements.

5) Retention of data – Pierre Fabre Medicament retains the Study report for 25 years from the end of the study for the reasons better outlined below. In any case, at the end of this retention period, data will be erased or irreversibly anonymized or aggregated.

How does the life cycle of data and processes work?

1. Data collection and data entry are performed by investigators
2. The EDC performs pseudonymization by providing a unique patient number for each patient entered in the EDC
3. Data cleaning by investigators and Fortrea
4. Data analysis by Fortrea
5. Study report writing by Fortrea
6. Aggregated data study report sent to Pierre Fabre Medicament

7. Pierre Fabre Medicament archiving for 25 years as from the end of the study

What are the data supporting assets?

Personal data will be processed through the following systems:

- eCRF (electronic Clinical Report File) stored on Medidata servers as EDC
- EDC extracts are shared on Fortrea's Share Drive and if needed shared with Pierre Fabre Medicament on the MFT based on the stat DTA.
- Analyses are performed and data for analyses are hosted by the SAS Hosted Environment with analyses conducted on SAS Enterprise Guide (i.e., SAS v9.4 or later).
- CSR writing will be on Fortrea servers.
- Pierre Fabre Medicament's SharePoint VINOREAL Study, which contains the study documents used only with Pierre Fabre Medicament's internal stakeholders on a strictly need-to-know basis.
- Pierre Fabre Medicament's Sharedoc which is used by Fortrea to share the statistical analysis (e.g., tables, figures and listings) with Pierre Fabre Medicament. Access to such system is granted by Pierre Fabre Medicament to Fortrea who uploads the analysis only.
- ZEC Pierre Fabre Biometrie, which is used by Pierre Fabre Medicament only for archiving the Study documents.

The CRO will ensure that the CRFs are securely stored at the CRO's research location in encrypted electronic form and will be password protected or secured in a locked room to prevent access by unauthorized third parties.

Fundamental principles

Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

The objective of the data processing is mainly to describe the current real-world effectiveness and safety data of OV-based treatments as well as the patient's healthcare pathway and quality of life (QoL) associated with this treatment of patients with ABC using FACT-B, PPQ, and WPAI questionnaires.

What are the legal basis making the processing lawful?

With specific reference to Italy, Pierre Fabre processes Patients' personal data on the basis of:

- the Patient's prior consent pursuant to Article 9(2)(a) of the GDPR for special categories of personal data (e.g., health data and adverse processing events). This consent is provided in addition to the Informed Consent Form ("ICF") that the Sponsor requires from Patients to agree to participate in the Study. In particular, the site will provide patients with a written notice on the processing of personal data in the context of the study prior to the extraction of data from patient records. If patients agree to participate in the study, they will also be asked to provide written consent for privacy purposes.

(i) consent given by their successors in title to whom the Privacy Policy may be made available and the relevant informed consent form may be signed by a successor in title, legal representative or anyone acting on behalf of the deceased person as their representative; or

(ii) (ii) only in the event that it has not been possible to obtain consent to the processing of data from their successors in title, on the basis of art. 110 of the Privacy Code, which provides that, if it is not possible to contact the data subjects to obtain consent or this involves a disproportionate effort or the risk of compromising the purposes of the Firm, the data controller must obtain the reasoned favourable opinion of the competent ethics committee, make public a data protection impact assessment and communicate it to the Guarantor for the protection of personal data, in accordance with the provision of the Guarantor of 9 May 2024.

Therefore, with reference to deceased patients, the legal basis of the processing is consent if the assignees can be contacted, and Article 110 of the Privacy Code otherwise. In order to contact the beneficiaries of deceased patients, Pierre Fabre makes reasonable efforts to verify whether the Site is able to contact them. Only in the event that these attempts to contact us are unsuccessful, Pierre Fabre, in application of Article 110 of the Privacy Code, will publish a notice on its website and on the website of the Centre, also requesting that it be posted in the Centre's waiting room where possible.

- Legitimate interest of the data controller (for Algerian and Chinese sites) as resulting from the knowledge of life conditions of individuals under treatment for data processing related to the Study,
- Execution of the contract with Study sites (investigators),
- Legal obligation for vigilance activities

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

All the data collected are adequate, relevant and limited to serve the objectives of the Study, which are the following:

The objective of the Study is to describe the current real-world effectiveness and safety data of OV-based treatments as well as the patient's healthcare pathway and quality of life (QoL) associated with this treatment of patients with advanced breast cancer.

- Primary objective:
  - To describe the effectiveness in terms of progression-free survival (PFS) at 2-years follow-up of OV-based treatment in patients with ABC, in both retrospective and prospective cohorts.
- Secondary objectives:
  - To describe the effectiveness in terms of overall survival (OS) at 2-years follow-up of OV-based treatment in patients with ABC in both retrospective and prospective cohorts.

- To describe the effectiveness in terms of PFS and OS of OV in patients with ABC in the retrospective cohort.
- To describe the clinical and demographic characteristics and comorbidities of patients with ABC treated with OV-based treatment in any line of treatment in a real-world setting and according to the molecular markers (HR status, HER2 status) in both retrospective and prospective cohorts
- To describe the safety profile as observed and the frequency of relevant Adverse Events (AEs) in patients with ABC treated with OV-based treatment in any line of treatment in both retrospective and prospective cohorts.
- To describe real-world treatment patterns (including prior anti-cancer treatment for breast cancer) of patients with ABC treated with OV-based treatment in any line of treatment, including treatment dose, treatment duration, permanent and temporary discontinuations, reasons for discontinuations and concomitant treatments in both retrospective and prospective cohorts.
- To describe the healthcare access and pathway of patients with ABC treated with OV-based treatment in any line of treatment assessed through hospitalizations, radiotherapies, and surgeries in both retrospective and prospective cohorts.
- To assess the evolution of QoL of prospective patients with ABC treated with OV-based treatment in a real-world setting by using the Functional Assessment of Cancer Therapy - Breast (FACT-B), an instrument that measures breast cancer patient's health status.
- To assess the preference of prospective patients with ABC for route of OV administration, by using a patient preference questionnaire (PPQ).
- To assess the impact of cancer on the work productivity and daily activities of prospective patients with ABC treated with OV for any line in treatment in a real-world setting by using the Work Productivity and Activity Impairment (WPAI) questionnaire.

Are the data accurate and kept up to date?

The source of data to be reviewed during study will include the patients' medical records, questionnaires (if applicable), original laboratory test, histology, and pathology reports.

The CRO has ultimate responsibility, on behalf of Pierre Fabre Medicament acting as Sponsor, for the collection and reporting of all clinical, safety, and laboratory data entered on the eCRFs and any other data collection forms (source documents) and ensuring that they are accurate, authentic/original, attributable, complete, consistent, legible, timely (contemporaneous), enduring, and available when required.

In particular, the eCRFs are approved with an electronic signature (changes to data previously submitted, will require a new electronic signature to acknowledge/approve the changes). Data entered into the eCRF will be reviewed for consistency by the data manager using both automated logical checks (i.e., issuing in automatic queries generated by the system) and manual review (i.e., issuing in manual checks set by the data manager or the monitor into the eCRF). For each detected inconsistency, an eCRF specific query will be generated (automatic or manual) and the investigator or data entry specialist will be responsible to correct or update any information that is incorrect or incomplete. To minimize the number of missing data, a specific query will be generated (automatic or manual) in order to confirm that data is truly

missing rather than being an overlooked entry in the eCRF. An audit trail within the system will track all changes made to the data.

The CRO or the sites are responsible for verifying the eCRFs at regular intervals throughout the Study to verify adherence to the protocol and Sponsor applicable SOP, completeness, accuracy and consistency of the data, and adherence to local regulations on the conduct of clinical research.

During and/or after completion of the Study, quality assurance auditor(s) named by the Sponsor or the regulatory authorities may perform on-site audits, also inspecting the various records of the Study (e.g., e-CRFs and other pertinent data) provided that patient confidentiality is respected.

What are the storage duration of the data?

Data Controller storage duration is 25 years from the end date of the Study.

Local storage for each study center is 15 years (subject to local variation to comply with local regulation) from the end date of the Study.

Fundamental principles

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

Pierre Fabre Medicament provides a privacy information notice as per Article 13 of the GDPR to patients participating in the Study and providing their consent in the manner and modalities provided for by the Guidelines for Data Processing within the Framework of Clinical Drug Trials – 24 July 2008 [doc. web. no. 1671330].

In certain cases (e.g., deceased patients), however, Pierre Fabre Medicament is exempted from the obligation to provide directly to data subjects a privacy information notice since this would represent a disproportionate effort according to Article 14(5) and recital 62 of the GDPR. This provision clarified that: *" However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration."*

Indeed, it should be noted that contacting interested parties for the purposes of the study would entail a disproportionate effort for Pierre Fabre for the following reasons:

(a) the study is to be conducted retrospectively in patients who started treatment with OV for advanced breast cancer, between 2011 and 2020; and

b) the estimated maximum number of subjects involved is up to 130 retrospective patients who in most cases could have died during clinical treatments.

With regard to the guarantees put in place by Pierre Fabre pursuant to art. 44 paragraph 1 of Law no. 56 of 29/04/2024, the above reasons must be considered as reasons of organizational impossibility to inform the patients concerned, as provided for by the Privacy Authority in its Provision of 9 May 2024, : i) the failure to collect data relating to the patients concerned who cannot be contacted, compared to the total number of subjects to be enrolled in the study, would have significant consequences for the study in terms of the quality of research results; (ii) residually, contacting all the patients concerned would involve a disproportionate effort given the particularly large number of stakeholders concerned.

In any case, the Privacy Policy referred to in Articles 13 and 14 of the GDPR and relating to the processing of personal data carried out in the context of the Study will also be available to the beneficiaries of deceased patients on the Pierre Fabre website at: https://clinicaltrials.pierre-fabre.com/en/vinoreal/ together with this DPIA.

If applicable, how is the consent of data subjects obtained?

The investigator will inform alive patients (or next of kin/legal representative in case patient is deceased, if applicable) of the nature, purpose, and consequences of their participation. Patients (or next of kin/legal representative, if applicable) will be provided with the current approved Patient Information Form to read, and any questions that may arise will be addressed.

Patients (or next of kin/legal representative, if applicable) will be duly informed of the study's objectives and the possibility of refusing or stopping their participation in the Study without any prejudice to their relationship with the investigator and their medical management. Patients (or next of kin/legal representative, if applicable) will also be informed about their rights concerning the processing of their personal data. All applicable local laws, regulations and EC requirements will be strictly applied.

After agreement of participation from the patient (or next of kin/legal representative, if applicable), the investigator will be able to collect required baseline data into the eCRF.

The investigator will document, in the patient's medical file, the patient’s (or the next of kin’s legal representative’s) Informed Consent, refusal, non-opposition, or opposition to study participation, before data collection is performed (if applicable).

The investigator will complete a patient screening log to register all patients invited to participate and reasons for non-inclusion. The patient screening log will be used to assess the representativeness of the Study sample, and the data to be collected in that log may include patient’s age, breast cancer stage, reason for non-inclusion if applicable. The reason(s) for refusal to participate will be recorded for those who declined to participate in the Study.

How can data subjects exercise their rights of access and to data portability?

Patients may at any time exercise their privacy rights and, in particular:

- Right to access according to which patients are entitled to request access to their personal data (Article 15 of the GDPR) via the generic address of the Sponsor's Data Protection Officer (DPO) : dpofr@pierre-fabre.com

Patients from Italy may exercise data portability right (Article 20 GDPR) using the same email address above mentioned.

How can data subjects exercise their rights to rectification and erasure?

Patients may at any time exercise their privacy rights and, in particular:

- Right to rectification according to which patients are entitled to request that any incomplete or inaccurate personal data hold by Pierre Fabre Medicament is corrected (Article 16 of the GDPR);
- Right to erasure according to which patients are entitled to request the erasure of the data collected by the Sponsor, unless deletion is likely to make impossible or seriously jeopardize the achievement of the research objectives (Article 17 of the GDPR); and

To exercise such privacy rights, patients can:

1) Liaise with the Site, the Study doctor or the research team who will then redirect the issue to the Sponsor's Data Protection Officer, or

2) Directly contact the Sponsor's Data Protection Officer (DPO) by sending an e-mail to the following address: dpofr@pierre-fabre.com

For Italy and according to Article 2-terdecies of the Privacy Code, in the event of the Patient's decease, the aforementioned rights may be exercised by individuals with an own interest, or acting in their capacity as the patient's representative, or for family reasons worthy of protection. Prior to his/her death, the Patient may expressly prohibit the exercise of some of the rights listed above by his/her assignees by sending a written declaration to the Sponsor or the Site in the manner indicated above. This declaration may be revoked or modified later in the same manner.

In any case, only pseudonymized personal data will be processed for the purpose of the Study. Therefore, Pierre Fabre Medicament might not be able to respond to Data Subjects' requests where the answer to such requests require identifiable data.

How can data subjects exercise their rights to restriction and to object?

In accordance with the provisions of the GDPR, data subjects may exercise the following rights at any time:

- Right to restriction according to which patients are entitled to ask the Sponsor to suspend the processing of certain personal data, where (i) the accuracy of the personal data is contested by patients, for a period enabling the sponsor to verify the accuracy of the personal data, (ii) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead, and (iii) the Sponsor no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims (Article 18 of the GDPR).
- Right to object according to which patients can object at any time to the processing of their personal data. In this case no new data will be collected. (Note for Italy : as the legal basis is the consent of Patients, should Patients decide to participate in the Study, they will have the opportunity to withdraw their consent at any time, without affecting the processing of personal data carried out before the withdrawal of the consent. In this case, no more data will be collected.

Are the obligations of the processors clearly identified and governed by a contract?

A master contract has been signed by and between Pierre Fabre Medicament (acting as Data Controller) and Fortrea (acting as Data processor) on 20 April 2023 (Document reference: CRO 2023-00329_NIS Navelbine_728094_Services Agreement_Final).

In the case of data transfer outside the European Union, are the data adequately protected?

In the case of data transfer outside the European Union, all collected data are duly protected (i) by the conclusion of Standard Contractual Clauses (SCC) as enacted by the European Commission (June 2021 edition) in case of transfer of data outside the European Economic Area ("EEA") and to a country not approved by the European Commission as providing adequate protection pursuant to Article 45 of the GDPR or (ii) through one of the derogations for specific situations as listed in Article 49 of the GDPR.

Risks

A) Evaluation of the risks to the rights and freedoms of the data subjects (Section 37, paragraph 7, letter c) of the GDPR) The main and major risks identified are the following ones :

- Illegitimate access to data
- Unwanted modification of data
- Data disappearance

There are no health related risks of taking part in the Study. In particular, the Study will not involve any changes in the local care standards of the Study subjects, will not compromise their physical or psychological integrity and will not require any special follow-up visits for these Study subjects.

However, the data processing deriving from the process described above may entail the following risks for Data Subjects' rights and freedoms:

a) the access to Study subjects' personal data without their awareness, including data related to health, and the related loss of confidentiality; and

b) the use of personal data for purposes other than those of the Process.

In general, sources of risk for personal data processed for the purposes of the Process may include:

a) either internal sources, operating – accidentally or intentionally – inside Data controller, such as employees, users and/or IT administrators of Data controller;

b) or external sources, operating - accidentally or intentionally - outside Data controller, including non-human sources, such as competing agents, water, dangerous materials, generic computer viruses, computer attacks, etc., or external sources, such as the Company's IT system.

In light of the risks listed above, the potential impacts on the data subjects involved that – depending on the classification of the different levels of severity provided for in the Annex 1 to this Data Protection Impact Assessment – could occur as a result of the Process are the following:

a) Data Subjects may face consequences that could be significant and they may overcome with real and serious difficulties according to severity level 4, in case of
   - Feeling of invasion of privacy and fundamental rights (e.g. discrimination);

b) Data Subjects may face serious disadvantages, which they may overcome despite some difficulties according to severity level 3, in case of
   - Problems relating to personal or professional knowledge (e.g. image, damaged reputation, loss of recognition);
   - Feeling of invasion of privacy without irreversible damage; and
   - Minor but objective psychological illnesses (defamation, reputation).

However, the processing deriving from the process involves a low risk to the rights and freedom of data subjects, since Data controller – also through the CRO – implemented appropriate technical and organizational measures as indicated below.

Furthermore, Data Subjects may benefit from the process, since it may lead to an improved understanding of Study subjects' illness and diseases. In particular, the findings from the Study may provide healthcare providers with important information for treating Advanced Breast Cancer (ABC) patients in the future.

Below are listed the technical and security measures set up by both the Sponsor acting as Data controller and the CRO acting as Data processor to manage and mitigate these risks, to avoid any data privacy issue.**B) Measures aimed at mitigating the relevant risks (Section 37, paragraph 7, letter d) of the GDPR)**

1. Data Storage Site Security

The sites where the Study data is stored, including data centres, offices, and off- site storage facilities, will have appropriate physical security controls.

- Data center spaces are continually monitored by on-site security teams and remotely by data center staff using recording webcams trained at all ingress/egress locations and numerous internal and external viewpoints and have controls in place to restrict and monitor physical access, requiring either multifactor or biometric authentication to enter.

2. Network Security

The networks on which the Study data will be transmitted will be protected from unauthorized access or infiltration, either internally or externally.

The measures that will be taken to ensure this will include:

- **Running periodic external and internal vulnerability scanning** Maintaining perimeter defences such as firewalls, intrusion prevention / detection systems and data loss prevention solution. Firewalls and related network security devices are hardened to meet standards-based industry best practices, and maintained in a change-controlled state to ensure that only minimum ports are opened for communications.
- Maintaining internal defences such as security information event management to analyse log files to identify anomalous behaviour and other threats, as well as network segmentation coupled with IP packet-level traffic monitoring.
- Inventory and change-control of network security devices within a configuration management database, including periodic discovery and confirmation of hardware devices.

3. Platform Security

The technology on which the Study data is stored, including servers, workstations and laptops, cloud service and other portable media will be protected from known threats by:

- Ensuring anti-virus or anti-malware systems are implemented and kept current for all operating systems.
- Ensuring server and endpoint operating systems have secure configurations to meet standards-based industry best practices and maintained in a change-controlled state.
- Ensuring vendor recommended security patches for both applications and operating systems are applied in a timely period, encrypting laptop hard drives and portable media.

- Ensuring risk assessments are performed on cloud providers using industry accepted methodologies such as Cloud Security Alliance or equivalent. SSAE16, ISO 27001 or other independent reports provide assurance on security controls and must be assessed when available.
- Ensuring mobile device management software is used to administer security controls on corporate supplied and bring your own devices.
- User endpoints (workstations, laptops, mobile devices) are encrypted, and data backups are encrypted in transit and in storage at the secondary data center.
- New systems are required to consider encryption of data at rest where appropriate (AES 256, SHA 2 standard). Key legacy systems have either already been retrofitted for encryption at rest or are in progress for retrofit.
- Storage subsystems are architecturally segregated from the application layer in the vast majority of systems.
- Clinical and diagnostics applications are designed and tested to ensure appropriate application technical controls to protect data. Clinical (GxP) systems are validated for intended use to comply with 21 CFR Part 11 and predicate FDA rules and analogous global regulations; validation affords an extra layer of assurance of security controls, including the protection and audit trail of sensitive data.
- Use of GxP Periodic Review procedures to verify that clinical systems are maintained in a validated state over their lifespan.
- A secure software development lifecycle and supporting processes, that require a security architecture review and vulnerability scanning to verify secure coding practices for web applications (OWASP Top 10).
- Host-based and application vulnerability scanning that require scheduled and/or pre-release testing to identify vulnerabilities. Vulnerabilities must be remediated within a procedurally defined time period based on criticality.
- Patch management practices to ensure firmware/OS/DB patches are applied in a timely manner; timeframes procedurally defined based on patch criticality.

4. Data Confidentiality

The confidentiality of the Study data will be maintained by protecting such data wherever it is stored, and whenever it is transmitted. These processes and procedures include:

- Maintaining separate databases for different types of data and limiting access to each database to those who may have a business need for such access.
- The use of industry accepted strong encryption and pseudonymisation.
- The secure disposal of paper, equipment, media and data.
- The security of data in transmission by means of encryption.
- Segregation of environments (e.g., production/test/development environments are controlled and maintained separately; production data is not permitted in lower environments; code migration responsibilities are isolated to preserve change control).

5. Data Access

The Study data will be accessed only by the authorized personnel of both Data controller and Data processor through such means as:

- The use of unique usernames and passwords to access the IT systems that host the Study data . Use multiple factors of authentication to access IT systems remotely.
- Implementing security policies to ensure that passwords are not shared and that systems' passwords are changed periodically in line with recommended best practice.
- Ensuring access to the Study data is authorised and approved.
- Ensuring access is granted on a least privilege basis.

- Terminating access where appropriate.
- Segregation of duties between users (e.g., use of security role assignments to ensure that data access is restricted based on employee responsibilities to the minimum required; separation of administrator/super user/end user roles).
- Centralized onboarding, job change, and off-boarding procedures to promptly add, modify, remove access to both the company network and individual applications.
- Periodic user access reviews to ensure effectiveness of the user add/modify/removal processes at the network and application levels.
- Standards-based IT network, server, database, and application hardening practices that enforce and document the configuration of equipment and software that provide access to company data.

6. Data Processing

Both the Data controller and Data processor will ensure that appropriate aspects of good security practice are enforced when processing any of the Study data. These processes include:

- Maintaining and enforcing policies on the secure handling and care of data and taking steps to ensure that such policies are known to all employees through awareness training.
- Ensuring that developers are trained and kept up to date in security coding techniques.
- Use of a configuration management database and configuration/change management processes to control the network, server, application and storage environments.

7. Data Backup, Disaster Recovery and Business Continuity

The continuity of access to the Study data will be maintained by ensuring standardized backup and recovery practices are in place, secured appropriately in transit and at rest, and supported by technical and organizational continuity plans and testing to ensure recoverability without compromising the security of sensitive data. These practices include:

- Maintaining standardized IT backup practices, using defined processes and configured tools to produce incremental and full backups of file shares, databases, applications and storage media containing company and client data.
- Ensuring that backup records are encrypted in transit and at rest while stored within a geographically distant secondary location secured to the same standards as the primary location.
- Periodically testing the restore function to ensure that backup files are and remain usable throughout their retention.

- Maintaining appropriate IT disaster recovery plans and recovery systems, and periodically testing these plans with supporting documentation to ensure that these plans are adequate to restore/recover/failover IT systems to an operational state, with data restored to pre-failure state, within appropriate recovery time and recovery point objectives (RTO / RPO) that are appropriate for the business criticality and sensitivity of the data in question.
- Maintaining appropriate business continuity plans for critical business functions, and periodically testing these plans with supporting documentation to ensure that these contingency plans are adequate to ensure continuance of business while recovering from catastrophic loss of normal business operations.

B. ORGANISATIONAL SECURITY MEASURES

1. Staff and 3rd Party Security Procedures

Both the Data controller and the Data processor will ensure and maintain the integrity of their respective personnel accessing the Study data by:

- Performing background checks on potential employees who will have access to personal data.
- Maintaining and enforcing policies on the secure handling and care of data and taking steps to ensure that such policies are known to all employees.
- Provide regular training to employees on privacy and security policies and security awareness.
- Ensure employees and contractors sign confidentiality agreements, or otherwise be under an obligation of confidentiality, prior to accessing the data exporter's data.
- Reviewing any subprocessors which the Data controller or the Data processor will use, to ensure appropriate security measures are in place.
- Ensuring the third party adheres to the minimum set of controls respectively prescribed by either the Data controller's or the Data processor's information security policies.

2. Data Subject Rights

Both the Data controller and the Data processor have established a set of data subject right procedures to fully comply with provisions of Article 15 to 22 GDPR included.

3. Data Breach Procedures

Both the Data controller and the Data processor have established a set of data breach security procedures that include the following elements:

- Detection: Establishing the facts of the incident and creating a diagnostic, containment and communications plan with respect to those whose data has been affected.
- Containment: Limiting the extent of the data compromise.
- Eradication: Removing all aspects of the hostile code/configuration, if applicable.
- Recovery: Restoring data and system to a known good state, without vulnerability.
- Review: Assessment of how to avoid similar incidents in future.
- Notification: Informing relevant interested parties of the data breach within legal and industry acceptable obligations and timeframes.

More specifically, regarding Italy:

as already specified in this document, with the recent amendment of Article 110 of the Privacy Code, for the processing of personal data concerning medical, biomedical and epidemiological research, in cases where it is impossible to obtain the consent of the data subject, the obligation of prior consultation with the Data Protection Authority has been replaced with compliance with the guarantees identified by the Data Protection Authority, pursuant to Art. 106 paragraph 2, letter d) of the Privacy Code, and also provided for by the deontological rules defined by the Guarantor for public and private entities, relating to the processing of data for statistical or scientific research purposes, aimed at identifying adequate guarantees for the rights and freedoms of the data subject, in accordance with Art.89 GDPR.

In light of this, the DPO recommends monitoring the activities of the DPA aimed at adopting deontological rules applicable to the study covered by this DPIA; if future ethical rules entail the need to modify some aspects of the processing put in place, the Data Controller must immediately comply with these provisions and update this DPIA

Date : 30-août-2024 | 16:55:55 CEST

Signature : DocuSigned by:
Pierre-André Poirier
EB9EFD9AD54B461...

Pierre-André Poirier

Data Protection Officer

ANNEX 1

Table on risks scenarios

Severity	Generic description of impacts (direct or indirect)	Physical damages	Emerging damages	Loss of earnings	Discrimination or stigmatization	Damages to identity	Reputational damages	Anxiety/Fear
5	Data subjects may have significant, or even irreversible, consequences that they may not overcome	- Death - Injuries with fatal consequences - Long-term disability - Permanent loss of physical integrity	- Financial risk - Substantial debts	- Inability to work - Inability to move - Loss of evidences in the context of a litigation - Loss of access to vital infrastructure (water, electricity)	- Loss of parental relationships - Kidnapping in person	- Criminal sanction - Change of administrative status and/or loss of legal autonomy (protection)	- Total loss of good reputation - Inability to find an employment	- Death by suicide - Long-term or permanent psychological disorders
4	Data subjects may face consequences that could be significant and they may overcome with real and serious difficulties.	- Serious physical illnesses that cause long-term damages (e.g. deterioration of health due to improper treatment or underestimated/ignored contraindications) - Long-term or permanent physical upsets (e.g. due to non-respect of contraindications) - Alteration of physical integrity e.g. after an attack, an accident at home, work, etc.	- Misappropriation of uncompensated money - Non-temporary financial difficulties (e.g. loan obligation) - Property damage - Loss of accommodation - Separation or divorce - Financial loss as a result of fraud (e.g. after a phishing attempt) - Locked abroad - Loss of customer data	- Loss of employment - Missed, unique and non-recurring opportunities (e.g. home loans, rejection of studies, internships or employment, prohibition of examinations)	- Victim of blackmail - Cyber bullying and harassment - Dismissal	- Feeling of invasion of privacy with irreversible damages - Feeling of violation of fundamental rights (e.g. discrimination, freedom of expression)	- Severe damage to the image - Damage of credit position	- Serious psychological syndromes (e.g. depression, development of phobia) - Feeling of vulnerability after a court call
3	Data subjects may face serious disadvantages, which they may overcome despite some difficulties	- Temporary disability - Lack of care leading to minor but real harm (e.g. disability) - Defamation that produces physical retaliation	- Refusal of access to administrative or commercial services - Increased costs (e.g. higher insurance prices)	- Lost career promotion - Outdated data (e.g. previous positions)	- Intimidation on social networks - Online advertising targeted on a private aspect that the individual	- Feeling of invasion of privacy without irreversible damage	- Problems relating to personal or professional knowledge (e.g. image, damaged reputation,	- Defamation that produces psychological retaliation - Refusal to continue using

Severity	Generic description of impacts (direct or indirect)	Physical damages	Emerging damages	Loss of earnings	Discrimination or stigmatization	Damages to identity	Reputational damages	Anxiety/Fear
					wanted to keep confidential (e.g. pregnancy advertising, drug treatment)		loss of recognition) - Online advertising targeted on a private aspect that the individual wanted to keep confidential (e.g. pregnancy advertising, drug treatment)	information systems (notices, social networks) - Minor but objective psychological illnesses (defamation, reputation)
2	Data subjects may face some drawbacks, which they may overcome with little difficulty	- Superficial injury - Less physical disturbance (e.g. mild illness due to non-respect of contraindications)	- Termination of an online account - Blocked online service accounts (e.g. games, administration)	- No possibility to contract with air carrier in case of card cloning	- Jokes from family and friends	- Feeling of invasion of privacy without real or objective damages (e.g. commercial intrusion)	- Receipt unsolicited targeted messages that could damage the reputation of stakeholders	- Temporary periods of high stress - Fear of using credit cards, online services - Loss of comfort (i.e. loss of leisure time, holidays)
1	Data subjects may face certain drawbacks, which they may overcome without any problem	- Very slight injury - Lack of adequate care for a dependent person (minor, protected person) - Temporary headaches	- Loss of time in repeating formalities or waiting for them to be completed - Receiving junk mail (e.g. spam) - Reuse of data published on websites for targeted advertising (information to social networks, reuse for paper mailings) - Targeted advertising for common consumer products	- Loss of time in repeating formalities or waiting for them to be completed - Lack of possibility to pay the utilities following, for example, the cloning of the credit card	- Lack of respect for freedom of online surfing due to denial of access to commercial sites (e.g. alcohol for wrong age)	- Simple annoyance caused by information received or requested	- Simple annoyance caused by information received or requested - Finding personal information of a common nature disclosed in a way that is not consistent with reality	- Fear to loss control on own data

Severity	Generic description of impacts (direct or indirect)	Physical damages	Emerging damages	Loss of earnings	Discrimination or stigmatization	Damages to identity	Reputational damages	Anxiety/Fear
0	No damages for data subjects	No physical damages for data subjects	No emerging damages for data subjects	No loss of earnings for data subjects	No discriminations or stigmatizations for data subjects	No damages to identity for data subjects	No reputational damages for data subjects	No anxiety/fear for data subjects