Data Protection Impact Assessment (DPIA)

Controller details

Name of controller	BeiGene (Italy) S.r.l.
Subject	DPIA: BGB-3111-MA-IT-401
Controller contact	privacy@beigene.com BeiGene (Italy) S.r.l. c/o BeiGene Switzerland GmbH Attn: Data Privacy Office Aeschengraben 27 21st Floor, 4051 Basel, Switzerland

1: Identify the need for a DPIA

The present data protection impact assessment ("DPIA") is aimed at assessing the risks to individuals enrolled in the Phase 4 clinical research study ("Study") sponsored by BeiGene (Italy) S.r.l. ("Sponsor"), Protocol ID: BGB-3111-MA-IT-401.

This Phase 4 observational study will investigate the outcomes of patients treated with zanubrutinib. The study includes both retrospective and prospective components:

- **Retrospective:** This portion will analyze data from patients previously treated with zanubrutinib under a compassionate use program. Importantly, this analysis will include all patients treated, regardless of their current status (e.g., lost to follow-up, deceased). This approach is crucial for accurately characterizing the overall treatment outcomes.
- **Prospective:** This portion will follow patients currently undergoing treatment with zanubrutinib, collecting data on their ongoing experience and outcomes.

The primary objective is to assess the effectiveness and safety profile of zanubrutinib in real-world clinical practice. Secondary objectives, as detailed in the study protocol, may include explorations of specific subgroups, long-term outcomes, and comparisons to other treatment options.

The Study will be conducted in accordance with the Clinical Trial Protocol (or "protocol"), the Participant Information Leaflet and Informed Consent Form ("ICF"), which are part of the documentation submitted to the Ethics Committee and the National Register of Observational Studies of the Italian Medicines Agency ("AIFA"). All data collected will be handled in accordance with established clinical trial data management standards.

A DPIA is considered necessary to assess the risks associated with: (a) the processing of pseudonymized patients' sensitive personal data (i.e., special categories of personal data), in the context of research projects or clinical trials; (b) cross-border transfers of pseudonymized patients' sensitive personal data.

2: Description of the processing

Nature of the processing.

Nature of processing: The investigator (or Study doctor) at the Study site, and other Study site staff collects and processes personal data of patients enrolled in the Study for the purpose of conducting the Study in accordance with the Protocol.

Source of personal data: Personal data is collected directly from the data subject or, in the case of medical history related to their disease, from their physician.

Data storage: Source personal data is stored at the Study site premises. Pseudonymized personal data is stored on Sponsor's premises. Sponsor's storage systems are ISO 27001 certified, meet the requirements of the US FDA's 21, part 11 standard and have an audit trail. All data is stored in encrypted systems with access limited to those with a "need to know". Regular vulnerability testing is performed against Sponsor's systems, and all systems are backed up regularly to protect against loss, alteration, or destruction of data.

Data sharing: The Study investigator and site personnel collect the patient data, store the source documents, and maintain the key linking the patient ID # to the patient's identity. When they share data with the Sponsor, they must use only the specific forms and clinical study systems, (e.g., the EDC system and secure file transfer platforms) designated by the Sponsor for sharing personal data and do not share the patient identification key. Such data is shared only in pseudonymized form (i.e. only using the patient ID #).

Pseudonymized patient personal data obtained during the Study may only be shared with the Sponsor (data controller), its vendors (appointed as data processors, as appropriate), and other third parties as permitted by the ICF and the protocol, unless permitted or required by law, including:

- The regulatory authorities in the EU and other regulatory authorities outside the EU overseeing the study in the countries where the Sponsor is seeking approval for zanubrutinib.
- The Sponsor's affiliated companies and representatives, including any laboratories and other vendors supporting with the conduct of the Study.
- The Independent Data Monitoring, the Scientific Steering Committee, and the Independent Review Committees monitoring the data from this Study.

Under the law, some parties will be permitted to access patients' uncoded personal data to verify the accuracy and validity of the Study or to meet other regulatory obligations. These parties are committed and contractually bound by confidentiality.

These parties include:

- The regulatory authorities in the EU and other regulatory authorities outside the EU overseeing the study in the countries where the Sponsor is seeking approval for zanubrutinib.
- Monitors and auditors appointed by the Sponsor.
- Sponsor's insurance company, in the event of an injury claim.

Processing identified as likely high risk:

- Processing of special categories of personal data, including ethnicity, health, and genetic data within the conduct of the Study.

- Cross-border transfers of pseudonymized personal data within the conduct of the Study.

Scope of the processing.

Scope of processing

The scope of the Study is Italian, but results of the study may be used globally by the Sponsor. Patients enrolled in the Study are treated and located in Italy.

The Study will enroll approximately 250 patients, including up to 50 participants who will be exclusively involved in the retrospective component.

The following categories of personal data are collected from patients enrolled in the Study at the site:

(1) Name, surname and contact information.
(2) Gender, and date of birth.
(3) Health data, which includes detailed medical records describing disease the clinical characteristics of the disease, disease and treatment history, diagnosis and ongoing treatment, concurrent medications, including any side effects or safety event.
(4) Ethnic origin data.
(5) Social security number.

The investigator ensures that patients' confidentiality is maintained, and patient identity is protected from unauthorized disclosures. The above personal data is collected and processed at a Study site level and shared with the Sponsor only if the following requirements are met.

The investigator and Study site must ensure that any personal data that is transmitted to the Sponsor, or its vendors (data processors) is:

(1) required under the protocol, and
(2) appropriately de-identified (i.e., pseudonymized, or coded) to ensure the following information about patients are **not** shared:
    - names or initials (full or partial).
    - full dates of birth.
    - contact information (such as phone numbers or home or email addresses).
    - personal direct or indirect identifiers (e.g., hospital or medical record, government, health insurance, or financial account numbers) other than patient identification numbers assigned as part of this Study.
    - geographic identifiers smaller than a country, or local equivalent (such as city, county, zip code, or other equivalent geographic identifiers); or
    - information about marital status, family, or household members; employment, sex life, sexual preference, or other sensitive data, unless it is relevant to the Study (for example pregnancy during Study of the patient or their partner).

Personal data collected and processed is limited to what is strictly necessary required to fulfill the scientific purpose of the Study or to meet regulatory obligations.

Personal data will be collected and processed on a continuous basis during the execution of the Study and retained for any period required by law and for any additional period during which retention of personal data is necessary for the defined processing purposes.

Description of the context of the processing.
Patients who enroll in the prospective portion of the study and those in the retrospective portion of the study who sign the ICF decide to enroll in the Study on a voluntary basis after being duly informed by study doctors and receiving the relevant ICF. In order to ensure the scientific integrity of the study, compassionate use patients who have been lost to follow-up, who the Study doctors have been unable to contact after at least three (3) attempts, and patient who have died will be automatically enrolled in the retrospective portion of the study (as further described in section 4 below). Patients who are part of the compassionate use program who are contacted and decline to consent will not be enrolled in the study. Patients are owners of their personal data and can exercise their privacy rights anytime as provided in the ICF and explained in Section 4 of this DPIA. The exercise of patients' rights may be subject to Sponsor's legal obligations, for example when immediately deleting patient personal data may compromise the integrity of the Study. The processing activity follows the criteria, rules and procedures which are global standards for clinical research studies. Personal data is processed only by specifically trained personnel (Study investigator, Study site personnel and Study monitors) operating under the study protocol. Patient data: Patients' identity is known to the treating physicians and their Study team, but it will not be shared with the Sponsor. All patient data is linked to the patient through a patient ID number, and the site/investigator has the key that links the ID number to the individual patient. Neither Sponsor, nor any vendor receives a copy of that key. Sponsor's study monitor will visit the Study site to review protocol compliance and conduct source data verification, having access to the patient-level data. Patient-level data will not be shared externally with any other Sponsor representative and will not be copied or otherwise retained by the study monitor.

Purposes of the processing.
The processing is conducted for the purposes of scientific research in the area of public health, to monitor the safety and efficacy of the treatment for the patient, to meet the Sponsor's regulatory obligations, and to generate sufficient data to support marketing authorization of the drug. Patients who undergo this processing activity may contribute to the development of new medical treatments or diagnostics for the target disease, improved understanding of the safety or efficacy profile for zanubrutinib, and potentially improve their health status.

3: Consultation process

Consultation with relevant stakeholders.
Patients Patients from whom consent is obtained are duly informed and can seek clarification regarding the processing of their data. An online notice will be available on the Sponsor's website for patients who are enrolled after three (3) failed attempts to contact them. However, the determination of which data is required for the study is made by scientists who specialize in the area of treatment. Patient data will be collected according to these criteria to ensure Study results' reliability and integrity.

Information security experts

System security is established by Sponsor's information security team based on global standards for processing of clinical trial data. Sponsor's information security team consists of professionals in the sector.

Relevant vendors may need to assist based on their role in the processing, in accordance with their contractual obligations with the Sponsor, including, but not limited to the data processing agreement and relevant information security addendums. All the vendors are required to meet specific information security requirements. Audit and qualification processes are in place.

4: Necessity and proportionality assessment

Describe compliance and proportionality measures, in particular.

Lawful basis

Personal data is to be collected with the patient's consent, where possible. The personal data of patients who we are unable to contact will be processed on the basis of the scientific research exceptions under GDPR article 9.2 (i) & (j). The collection and use of personal data is also required to comply with legal and regulatory requirements, including requirements that the Sponsor shares personal data with regulatory agencies within and outside the EU that oversee clinical studies, drug safety, or review applications to market zanubrutinib.

Note on the retrospective component of the Study: As a standard procedure, the patient will receive a dedicated ICF describing the scope of the Study and will be able to freely agree to participate and consent to the processing of personal data. Notwithstanding the foregoing, in special circumstances, certain patients (i.e., compassionate use patients who have been lost to follow-up or who have died) may be unavailable to the Sponsor, and it may be impossible to obtain consent to process their personal data. This impossibility will be determined as the result of all reasonable efforts to contact living patients (including verification of their living status, consultation of data in their medical records, use of any telephone numbers provided, and obtaining publicly available contact information), and only then will it be determined that they are deceased or unreachable at the time of enrollment in the study.

In the event that it would not be possible to obtain the patient's express consent, under the specific organizational circumstances described above and defined in the "*Provvedimento n. 298 del 9 maggio 2024*" of the Italian Data Protection Authority, the Sponsor will process the patient's personal data by implementing appropriate safeguards to protect the patient's personal data during the conduct of the retrospective observational study as described in this DPIA.

Proportionality

The processing of patients' personal data achieves the Sponsor's purpose. There is no other way to achieve the same purpose than processing patients' personal data as described in the Protocol. The potential risk to the patient is minimal, given 1) the security protocols and access limitations established for the clinical data systems, 2) the pseudonymization of the data and data minimization steps reduce the risk of reidentification of the patient, and 3) all recipients of the data are bound by confidentiality obligations.

Data quality and minimization

Sponsor only collects data that is required to fulfill the scientific purpose of the Study or to meet regulatory obligations. Sponsor does not collect any direct or unique identifiers, such as the patient's

name, initials, address, contact details, or full date of birth as part of the Study. Data is always processed by Sponsor and its vendors in a pseudonymized form. Data that is collected is subject to a quality check to ensure that no patient identifiers were inadvertently sent to Sponsor, and Sponsor has a process in place to redact or destroy any inadvertent disclosures and retrain the sites. Access to personal data is provided on a "need-to-know" basis and organizational measures are in place (e.g., data segregation) to avoid access from unauthorized personnel.

Data subjects' rights

Patients can exercise their rights through the Study doctors at the site level. Patients have the right to request access to their personal data and, if applicable, ask for corrections. In certain circumstances, they have the additional right to object to how personal data is being handled, request deletion, restrict aspects of the collection and use of their personal data, or ask for a copy of personal data to be provided to them.

To exercise these rights, the patient can contact the Study doctor, who will route the request to the Study site and the Sponsor. The Study site and/or the Sponsor will consider and respond to the request in accordance with applicable laws. Should the patient contact the Sponsor directly, the Sponsor will ask the patient to direct their request through their study doctor, as Sponsor does not have access to the code linking the patient's ID # to the individual patient.

Relevant information about this process is provided to the patient in the ICF and, for patients who could not be contacted by the Sponsor, is available on the Sponsor's website, together with this DPIA.

Data processors

All vendors who process patient data must pass a strict IT security assessment, enter into a data processing agreement and, if located outside of the EU, must execute the EU's approved Standard Contractual Clauses. Vendors are subject to oversight by the Sponsor and are instructed not to collect any direct or unique identifiers, unless absolutely necessary to perform their services (e.g., travel vendors who need that information to book transportation or reimburse patients).

International Transfers

The Sponsor will only transfer patients' personal data outside of the EU where it has the legal right to do so. Personal data is transferred under the following criteria to ensure the highest level of protection for data subjects:

- Transfers to countries deemed by the EU to provide adequate protection under their local privacy laws.
- If the destination country doesn't hold this status, the Sponsor conducts a Transfer Impact Assessment. If the assessment identifies any outstanding risks, the Sponsor implements additional technical and organizational measures to ensure that the transferred data meets a protection level substantially similar to the EU.
- The Sponsor signs the Standard Contractual Clauses ("SCCs") with all vendors and third parties (other than health authorities) processing the data in a country not deemed adequate.
- In exceptional cases, when none of the above methods can be implemented, the Sponsor resorts to transferring the data for important reasons of public interest or by obtaining the explicit consent of the patients to transfer the data, thereby respecting their rights and autonomy over their personal data.

Notwithstanding the foregoing, the Sponsor adopts supplementary measures to those offered by the SCCs or by the other approved transfer mechanism relied upon to ensure an essentially equivalent level of protection under EU law, of personal data transferred outside the EU or the EEA. These measures include, but are not limited to, data minimization, data pseudonymization and other data security and data quality measures.

5: Identify and assess risks

Source of risk and nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Overall risk
(1) Inadvertent or inappropriate disclosure of personal data internally or externally due to a lack of appropriate controls being in place.	Possible	Significant	Medium
(2) Breach of data held electronically by "hackers" or other system failure.	Possible	Significant	Medium
(3) Information released in pseudonymized form might lead to disclosure of personal data if pseudonymization techniques chosen are not effective.	Remote	Severe	Low
(4) Data may be transferred to countries with inadequate data protection regimes.	Possible	Significant	Medium
(5) Loss of electronic equipment of Sponsor's personnel.	Possible	Significant	Medium
(6) Data may be kept longer than required in the absence of data retention policies.	Remote	Significant	Low
(7) Personal data used for purposes not expected by data subjects or not anticipated.	Remote	Significant	Low
(8) Genetic data may be used to identify an individual and to discriminate against said individual.	Remote	Significant	Low

6: Identify measures to reduce risk

Additional measures taken to reduce or eliminate identified risks					
Risk		**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
(1)	Inadvertent or inappropriate disclosure of personal data internally or externally due to a lack of appropriate controls being in place.	Measures are in place to ensure personal data are not disclosed to unauthorized personnel, including vendors and third-party stakeholders. These include internal policies and procedures, access controls and audit trails for all clinical systems, and training on all policies, procedures, and clinical systems. Sponsor has a rigorous process to monitor for inadvertent disclosures of data, ensure the disclosed information is destroyed and the person who inadvertently disclosed the data is retrained. Additionally, vendors are under contractual obligations to ensure the same level of protection of the personal data they process, and their systems and controls are subject to review and approval by Sponsor's information security team.	Reduced	Low	Yes
(2)	Breach of data held electronically by "hackers" or other system failure.	Information security team has implemented several technical measures, including firewall, endpoint security and potential threats are monitored through SIEM tool. Disaster recovery measures are in place. Sponsor is ISO 27001 certified and annual surveillance audits are performed. Dedicated training is carried out to employees.	Reduced	Low	Yes
(3)	Information released in pseudonymized form might lead to	Pseudonymization is the industry standard for protecting clinical data. To ensure reidentification is not possible, Sponsor does not collect any direct patient	Reduced	Low	Yes

	disclosure of personal data if pseudonymization techniques chosen are not effective.	identifiers and minimizes collection of indirect identifiers to those required. No patient names, initials, dates of birth, contact information, or unique identifiers (other than the patient ID #) are shared with Sponsor as part of the clinical trial. Further, even if hackers access the data, the reidentification key linking the patient ID # to the patient's identity cannot be obtained by hacking the Sponsor's or Vendors' systems.			
(4)	Data may be transferred to countries with inadequate data protection regimes.	Measures are in place to ensure that transferred data meets a protection level substantially equivalent to that within the EU and/or EAA as described in Section 4 of this DPIA.	Reduced	Low	Yes
(5)	Loss of electronic equipment of Sponsor's personnel.	Controls are in place to avoid data loss. All laptops are encrypted, and information security measures are in place to remotely wipe data from electronic devices and avoid data loss. Further, clinical data is stored on central servers and may not be downloaded to individual laptops.	Reduced	Low	Yes
(6)	Data may be kept longer than required in the absence of data retention policies.	Information governance and data retention policies are in place to ensure data is kept for the minimum time necessary for the relevant purposes. Data is retained in compliance with applicable laws and regulatory requirements.	Reduced	Low	Yes
(7)	Personal data used for purposes not expected by	Measures are in place to ensure the data subjects are informed of all uses for the data and an appropriate lawful basis in place.	Reduced	Low	Yes

	data subjects or not anticipated.	For example, relevant consent forms are provided to patients, separate consent is collected for the use of personal data for future research and systems are in place to track such consents. In cases where patients are unavailable to the Sponsor and unable to receive the ICF (as described in Section 4 of this DPIA), it's important to recognize that these individuals previously participated in a study or compassionate use program, and therefore received an initial ICF that outlined the possibility of future research using their data, with their consent if required. It is thus reasonable to infer that these patients would anticipate a similar use of their data for research purposes. In any case, Sponsor will make this DPIA together with its privacy policy available on its website. The Sponsor also has internal controls to ensure that future research consents are checked prior to further use of the data and staff are instructed to check with legal and compliance in the event they are uncertain whether the planned use is within the scope of future research described in the ICF.			
(8)	Genetic data may be used to identify an individual and to discriminate against said individual.	Measures are in place to ensure that genetic data is only transmitted and stored via secure systems and use of and access to data is strictly limited and monitored. Data on genetic mutation and gene expression are published in aggregate form and full sequence data are never shared. Large scale genetic libraries do not currently exist that would allow linkage back to an individual, even if the data were accessed.	Reduced	Low	Yes

7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Joseph Cook, Director, Privacy and Data Ethics, North America, Europe, and New Markets	N/A
Residual risks approved by:	Joseph Cook, Director, Privacy and Data Ethics, North America, Europe, and New Markets	N/A
DPO advice provided:	Joseph Cook, Director, Privacy and Data Ethics, North America, Europe, and New Markets	N/A
Summary of DPO advice: The DPO has assessed and identified the risks involved in the processing activities and has reviewed and approved all mitigation measures. DPO believes minimal residual risk to the data subjects remains after application of mitigation measures.		

Signed by:
Joseph Cook
Signer Name: Joseph Cook
Signing Reason: I approve this document
Signing Time: 04-Oct-2024 | 13:16:46 PDT
C6D6025FBFB74B059BF8CF3685082DCA

04-Oct-2024 | 13:18:14 PDT