onetrust

Assessment details

ID 122686

Name Italy_Study 224207 retrospective use of data_PIA

Organization Research & Development

Description

Date created 03/16/2026 03:48 PM

Deadline

Completed date 04/23/2026 01:14 PM

Date submitted 03/31/2026 08:50 AM

Last updated 04/23/2026 01:14 PM

Stage Completed

Approval stage

Status Active

Critical 0

High risks 0

Medium risks 0

Low risks 0

Total risks 0

Residual risk level None

Residual risk score 0.0

Result Approved

Primary record id 7655

Primary record name Italy_Study 224207 retrospective use of data

Template version 20

Open risk count 0

Open info request 0

Assessment questions

1 General Information

1.1 **What is the name of the business activity processing personal information?**
Please type the name of the activity in an understandable and recognisable way

Response

Italy_Study 224207 retrospective use of data | Research & Development

Justification

None

1.2 **Please describe the business activity processing personal information, including the purpose.**
Please describe the business activity in detail and how you intend to use the personal information of individuals to achieve your aims. Specifically:

- *What do you want to achieve?*
- *How are you going to achieve this?*
- *How will personal information be used to do this?*
- *What is the benefit to GSK and to the individual?*

Personal information is information that can be used to identify you directly or indirectly, on its own or when combined with other information.

Some examples of personal information are: Name / phone number / address / date of birth / bank account details / unique identifiers / social media posts / geotagging / staff number / IP address / video image

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

This assessment regards the processing of data for non-reachable patients for a multi-site retrospective, non interventional study.
The study is a multi-site retrospective, non-interventional chart review study that uses longitudinal, RWD from routine medical records, leveraging real-world data (RWD) from routine medical records to analyze data from adult patients who received belantamab mafodotin combination therapies among patients with multiple myeloma (MM) from first relapse (2L+) as part of Compassionate Use Programs (CUP) in Italy.
"Retrospective" means using data that was already collected in the past.
The CUP included a Name Patient Program (NPP). A NPP was opened once the results from the DREAMM-7 and DREAMM-8 studies were published. The requests for either belantamab mafodotin combination therapy (combined with bortezomib and dexamethasone (BVd) and pomalidomide and dexamethasone (BPd)) through NPP remained available until December 31st, 2025.
According to the Italian Medicines Agency (AIFA) guidelines on observational studies published in August 2024, data coming from Compassionate Use programs can only be gathered retrospectively.
The objectives of this study are to describe real-world treatment patterns with belamaf combination therapies (BVd or BPd), including description of starting dose and frequency of treatment in the Compassionate Use Programs.
The study does not impose a treatment protocol, any diagnostic/interventional procedure, or a visit schedule.
Individual-level data on patients with MM from first-relapse treated with belamaf combination therapies will be analyzed.
Eligible patients from Italian CUP will be included in the study.
The study will collect data of approximately 100 patients within the NPP.
Written informed consent (if required based on local regulatory and legal country requirements) will be obtained from all patients before enrolment into the study.
The name of the GSK legal entity who is sponsor for the study is GlaxoSmithKline LLC.
The process flow from chart review to data entry in the Electronic Data Capture (EDC) system involves the following steps and parties:
Chart Review and Data Extraction:
Site Investigators or designated site personnel review patient medical records to extract relevant data, including baseline characteristics, study outcomes, and other pertinent information. The medical record serves as the source document for this information.
Data Entry into Electronic Data Capture (EDC): Castoredc.com is the database used De-identified data (pseudo-anonymous to non-site staff) is transferred from the patient's medical record into the electronic Case Report Form (eCRF) within the EDC system. The EDC system is designed to minimize errors with built-in logic checks to prevent missing or illogical data.
Verification and Quality Assurance:
Site Investigators are responsible for ensuring the accuracy and timeliness of data entry.
Data Management and Storage:
All data extracted is stored on secure servers, ensuring compliance with local or national regulations.
Findings will be disseminated through scientific publications and presentations in an aggregated, anonymous manner.
Timelines
Start of data collection: Q4 2025
End of data collection: Q2 2026
Final report of study results: Q4 2026
The level of access to personal information (PI) for different study roles is as follows:
Study Staff:
Full access to personally identifiable information (PI) such as name, address, phone number, and health insurance number.
Responsible for collecting and storing PI securely at the study site.
CRO (MyTomorrows):
Access to coded data only.
Does not have access to direct identifiers like name or contact details.
GSK Team:
Access to coded data only.
Coded data is anonymized once the code list is destroyed, ensuring no linkage to the participant.
IRBs/IECs and Regulatory Authorities:
May review study records, including PI, to ensure compliance with legal and quality requirements.
Appropriate measures are taken to protect PI, and direct identifiers are never sent to GSK or CROs.
This questionnaire and the subsequent PIA are necessary to assess the feasibility to collect data for the Italian patients that are either deceased or not reachable and so their consent cannot be obtained, in compliance in particular to the Italian Privacy Code 101/2018 articles 110 and 110 bis.

Justification

None

1.3 **When is the expected start date of the activity?**

Select the date that the activity is due to start or started if the date is in the past.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

07/01/2025

Justification

None

1.4 **When is the expected end date of the activity?**
Select an end date if this is a one-off activity, project or initiative.
Select "Not Applicable" if this is an ongoing activity with no end date.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response
09/30/2026

Justification
None

1.5 **Is this a global or a local activity?**
A local activity involves one market.

A global activity will involve multiple (two or more) markets or personal Information of individuals located in multiple markets.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response
Global

Justification
None

1.6 **Which regions carry out this activity?**
Please select all regions that are involved in carrying out this activity.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response
Europe

Justification
None

1.10 **Who decides why and how personal information is processed as part of this activity? Please select the appropriate GSK entity for this activity.**
This is known as the controller in some jurisdictions.

If one entity is involved in determining the purpose and design of this business activity, please begin by typing the country it is associated with to filter the drop-down results.

If multiple entities are involved in determining the purpose and design of this business activity, please either select the specific entities or regions involved.

The regions available for selection are:

- *Africa*
- *Asia-Pacific*
- *Australia*
- *Canada*
- *Central America/Caribbean/Mexico*
- *Europe*
- *Middle East*
- *South America*
- *United States*

Please refer to guidance examples for controller and processor here.

Response
UK GSK | Privacy | United Kingdom
UNITED STATES GSK | Privacy | United States

Justification
None

1.11 **Who processes personal information as part of this activity but is not involved in deciding why and how personal information is processed? Please select the appropriate GSK entity(ies) for this activity.**
This is known as the controller in some jurisdictions.

If one entity is involved in determining the purpose and design of this business activity, please begin by typing the country it is associated with to filter the drop-down results.

If multiple entities are involved in determining the purpose and design of this business activity, please either select the specific entities or regions involved.

The regions available for selection are:

- *Africa*
- *Asia-Pacific*
- *Australia*
- *Canada*
- *Central America/Caribbean/Mexico*
- *Europe*
- *Middle East*
- *South America*
- *United States*
- *Not Applicable*

Please refer to guidance examples for controller and processor here.

Response
Not applicable

Justification
None

1.12 **Does the activity consist of any of the following high risk features or is there any other reason a Privacy Impact Assessment (PIA) is required?**
Some of these activities will trigger a PIA to be completed, others will only require a PIA when multiple activities are combined.

A Privacy Contact or Leader may ask you to complete a PIA in some circumstances where it is not automatically triggered.

Please hover over each option below to obtain a further explanation.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Processing of sensitive personal information | PIA is required by the Data Privacy Authority

Justification

None

2 Personal Data

2.1 **Please select the group(s) of individuals whose personal information will be processed. For each group, select the categories of information and individual data elements processed.**
Remember that any information that GSK could identify an individual through, directly or indirectly, on its own or in combination with other personal information we hold, should be selected.

Please include all the personal data elements that you reasonably expect could be collected for this activity.

Response

Patients

Sensitive Elements
- Ethnicity or Race
- Medical or Health Information

Restricted Elements
- Key Coded Data
- Age or date of birth
- Personal contact details

Basic Elements
- Gender or Title

2.2 **How many individuals' personal information will be used to carry out this business activity?**
Please estimate the number of individuals whose data is processed for this activity. If the activity does not have an end date, please provide an annual estimate.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

0-1000

Justification

None

2.3 **Where will the individuals be located whose personal information will be used for this business activity?**
Please select all locations individuals are located, you can select multiple options.

In certain jurisdictions, individuals will be referred to as data subjects.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response
Europe

Justification
None

2.4 **Please select the appropriate basis for processing the personal information.**
You must have a valid basis to carry out your business activity. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individuals.

If consent is only used as an appropriate condition for processing sensitive personal information, and not as a lawful basis, please only select consent in the following question.

If selected, please explain the legal obligation in the justification box including name of statute or regulation and section references where possible.

If selected, please explain the contractual obligation in the justification box including name or reference for the related contract(s), where possible.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response
Consent of the individual
Italian Privacy Code 101/2018 art. 110 and 110 bis. Garante's provision 10016146, dated 09May24

Justification
lawful basis for processing is the consent for the patients that are reachable.
For those subjects that are not reachable or deceased, the lawful basis for processing resides in the provisions of the Italian Privacy Code 101/2018 art. 110 and 110 bis and the Garante's provision 10016146, dated 09May24

2.5 **Please select the appropriate condition for processing the sensitive personal information.**
Sensitive personal information needs more protection because, due to its sensitivity, it poses a higher risk to individuals if it is misused.

You must determine an additional condition for processing sensitive information before you begin this processing.

Please hover over each option below to obtain a further explanation.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response
Explicit consent
Art. 110 and 110bis Italian Privacy Code; Garante's provision 10016146 of 09May24; GDPR: art 9.j and 89.1

Justification
None

Comments

Michaela Tutone *03/24/2026 03:15 PM*

The lawful basis for processing of reachable patients is the explicit consent of the individual. For the patients who are not reachable or deceased, the lawful basis for processing resides in the EU Regulation 2016/679 art 9, comma j, art. 89.1, as well as in the provisions of the Italian Privacy Code 101/2018 art. 110 and 110 bis and in the Garante's provision 10016146, dated 09May24

3 Necessity and Proportionality (of data)

3.1 **Describe the rationale for using the volume and categories of personal information selected**

Please explain why the number of information types and numbers of individuals involved are relevant and necessary to achieve the aims of this activity.

Response

The volume and categories of personal information used in this study are selected to achieve the study's objectives effectively as described in the study protocol. The study will be collecting relevant data from medical records for patients with multiple myeloma from first relapse, treated with belantamab combination therapy, as detailed in the study protocol.
Volume of data: A sufficiently large volume of data is necessary to ensure statistical validity and reliability of the study results to ensure an understanding of the characteristics of patients treated with belantamab combination therapies during the nominal use program in Italy.

3.2 **Could your objectives be achieved with less information from fewer individuals?**

Remember you should only use the information that you need. Please consider whether the same results could be achieved with less information.

Please explain your rationale in the justification box below.

Response

No

Justification

GSK ensures that only essential data is collected and processed. The data collected is limited to what is necessary to achieve the study objectives, in line with data minimisation principles.
The objectives of this study could not be effectively achieved with less information or fewer research subjects. The nature of these studies requires comprehensive data to ensure that the findings are statistically significant and applicable to a broad population. Reducing the volume of data or the number of participants could compromise the validity and reliability of the study outcomes.
By its nature, real-world data can be less complete and reliable, which is why often a larger population is needed to secure validity of the results.

3.3 **Is there any other way to achieve the purpose?**

Consider the balance between business benefit and the privacy of individual. Could you achieve a similar benefit to the business in a way that gives greater privacy to the individual?

Please provide your rationale in the justification box below.

Response

No

Justification

There are no alternative approaches that would achieve the same purpose without processing the personal data as currently done. The insights gained from real world data are crucial and cannot be achieved without processing personal data. The observational nature of NI studies relies on the collection and analysis of data to provide meaningful results.

3.4 **Is all the personal information collected necessary for the intended purpose?**

You should avoid collecting or using information because it is an easier option or because you might need it in future.

Do you need to use each personal information type you are collecting for this business activity?

Please explain your rationale in the justification box below

Response

Yes

Justification

Yes, GSK will ensure that each data element collected is essential for achieving the study objectives and ensuring the validity and reliability of the findings.

3.5 **Will the data collected be used for anything other than the specified purpose?**

Personal information should only be used for the purposes (e.g. business activities) for which it was collected. it should only be used for other purposes if they are compatible with the original purpose for which it was collected.

Consider whether any other GSK colleagues or teams have access to the data and be able to use it for their own purposes. Are these purposes compatible with or similar to the purposes for which it was collected?

Please explain your rationale in the justification box below if you select 'Yes'.

Response

No, the personal information will only be used for the purpose stated in question 1.2.

Justification

Personal data will be used according the information provided in question 1.2

4 Consent

4.1 **How do individuals provide consent for their information to be collected?**

Opt-in consent *requires user action to confirm they do want their data included and processed in this way, with data not processed unless confirmation provided. Examples of opt-in are:*

- *Signature box*
- *Tick box asks user to select to confirm they want their personal data used for this activity*
- *Verbal agreement (documented by GSK)*

Opt-out consent *tells individuals that their consent is deemed to have been given, unless there is user action to notify GSK that they do not want their data included in the activity, with data not processed only if notification provided. Examples of opt-out are:*

- *Tick box asks for user to select if they do not want their personal information used for this activity.*

Continuing without objection *is where an individual is deemed to have given consent unless they tell us otherwise. Examples include:*

- *Continuing to use a website after seeing a cookie pop up. (this would not be acceptable under the GDPR)*
- *"By using this site / continuing with this form you consent to..."*

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Opt-in | Italian Privacy Code 101/2018 art.110 and 110 bis, and in the Garante's provision 10016146 dated 09 May 2024

Justification

For patients who are not reachable or deceased, the lawful basis for processing their data resides in the EU Regulation 2016/679 art 9, comma J, art. 89.1, as well as in the provisions of the Italian Privacy Code 101/2018 art.110 and 110 bis, and in the Garante's provision 10016146 dated 09 May 2024.

4.2 **Can individuals change their consent preferences, for example withdraw their consent, at any time?**

Most privacy laws require that if an individual provides consent, they should be able to withdraw their consent in a way that is as easy as those for giving consent.

If individuals cannot change their consent preferences, please provide a rationale for why this is acceptable or an alternate approach to managing consent in the justification box below.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Yes

Justification

Reachable patients may withdraw consent; for those patients that are no longer reachable, we are assessing it with a DPIA as per the Italian DPA provision. For patients who are not reachable or deceased, the lawful basis for processing their data resides in the EU Regulation 2016/679 art 9, comma J, art. 89.1, as well as in the provisions of the Italian Privacy Code 101/2018 art.110 and 110 bis, and in the Garante's provision 10016146 dated 09 May 2024.

4.3 **How can the individual change their consent preferences?**

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Preference centre

Justification

None

Comments

Michaela Tutone *03/24/2026 03:26 PM*

Patients are instructed to contact primarily their site staff/physician. The option to change their consent preference is well described within the individual consent form for the study.

4.4 **What source do we obtain the personal information of individuals used in this processing activity from?**
Select one or more that apply.

Please hover over the options to see more information.

Please add any further relevant information to the justification box below.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Contracted third parties

Justification

The centers, as independent data controllers, collected patients' clinical data during NPP. As part of the Study, the Centers will be responsible for removing all patient identifiable information and will ensure that the data is pseudonymized in eCRF.

4.5 **Which system collects the personal information?**
Please select the system that collects the personal information from the individual, third party or other provider identified in response the previous question.

A GSK operated system/application in this context is one that supports information-related activities. This could include software systems, applications or databases.

If you can't find your system from the drop down list, please raise a ServiceNow ticket and this will be investigated for you.

Response

Chrd Veeva Vault Etmf | Privacy | Unknown

Justification

None

4.6 **Please select the third party the personal information is collected from, from the drop down list.**
If the third party is not available in the drop-down list, please select not sure and let your privacy lead or privacy contact know.

Response

Impatients N.V. (myTomorrows) - GZ - 29/11/22 | TPRM | Unknown

Justification

None

5 Individual Rights

5.1 **Can a copy of the personal information used for this activity be provided to an individual upon request?**
An individual may have the right to request a copy of their personal information in certain countries. For example, under the GDPR this is called a Data Subject Access Request and we have one month to respond. Email, excel, word, pdf, etc is an acceptable format.

Please use the justification box below to provide a rationale if 'No' is selected.

Response

Yes - information can be provided in a digital format (e.g. files, images, recordings, etc.)

Justification

In case of data collection by GSK, GSK has an Individual Rights Request ('IRR') process in place. Moreover, for study records, patients are invited (as specified in the ICF and privacy consent form) to contact their study staff. Data can potentially be provided in digital format.

5.2 **Is there a mechanism or process to ensure the personal information is kept accurate and can be updated when required?**

We must keep personal information accurate while we hold it. Please describe how we identify inaccurate personal information and correct it when it is inaccurate or out of date.

Response

Yes

Justification

Data collection process involves a level of data validation. Built in mechanisms exist to correct typing errors, field verification, data formats, range checking. Study specific checks, which are specifically programmed to verify whether the inputted data is correct, are put in place.

5.4 **Is there a process in place for when an individual asks for GSK to stop using their information?**

In some circumstances individuals may be able to ask us to restrict the use of their personal information. This means that GSK would be allowed to store the information but not use it.

Requests to restrict processing are most common when information is held longer than it should be or where there is a legal challenge.

If we had to stop using the personal information of one individual, could we continue the activity that their information was used for without impact?

Response

Yes

Justification

The study gathers data from electronic medical records provided to a third party in pseudonymized form. GSK does not hold identifiers and cannot trace or isolate individual records. Any data subject rights, including requests to restrict processing, must be managed by the original data holders (participating study sites). Reachable patients may withdraw consent contacting the study physician. Any restriction on use would need to be applied by the data holder and, if necessary, reflected in the data provided to us.

6 Access/Transfers

6.1 **Where/who might the personal information be shared to/with?**

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Other GSK owned entities | Regulatory Authorities and Ethics committees

Justification

1. Authorities (government agencies, tax authorities, law enforcement, regulators): Personal information may be sent to authorities such as government agencies, law enforcement, and regulators to comply with legal obligations and regulatory requirements. This includes reporting for public health purposes, responding to law enforcement requests, and adhering to regulatory standards for NI Studies (NI Studies can be part of regulatory package) and pharmaceutical operations. Sharing data with authorities is often mandated by law and is necessary to ensure compliance with statutory obligations and to support public interest activities.
2. Other Companies in GSK:
Personal information may be shared with other companies within the GSK corporate group to facilitate global operations, ensure consistency in research practices, and support collaborative projects. This internal sharing is governed by Intra Group Agreements that ensure compliance with data protection standards across all GSK entities. Sharing within the corporate group allows GSK to leverage resources and expertise from different entities while maintaining a high level of data protection.
3. Other organizations that provide services for GSK (e.g., vendors, suppliers, contracting agencies, advisers, etc.): These organizations are typically engaged under contractual agreements that include data protection clauses to ensure compliance with data protection laws. Sharing data with service providers is necessary to support various operational activities, including clinical trials, research, and business functions. It allows GSK to access specialized expertise and resources while ensuring that personal data is handled securely and responsibly.

6.6 **Please select any GSK legal entity(ies) with whom the personal information is shared?**

For support in identifying GSK legal entities, please speak to your Privacy Contact or Privacy Lead.

If you can't find the correct GSK legal entity from the drop down list, please raise a ServiceNow ticket at the following link and this will be investigated for you.

Response

UNITED STATES GSK | Privacy | United States | UK GSK | Privacy | United Kingdom

Justification

None

6.7 **Is personal information transferred from one country to another?**

Personal information is transferred when it is transmitted from one country to another across jurisdictional borders.

Please note, a transfer does not mean the same as transit. If personal data is just electronically routed through Country B, but the transfer is actually from one organisation in Country A to another in Country A and there is no intention that this information will be access or used whilst transiting through Country B, then it is not considered a transfer to another country.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Yes

Justification

None

6.8 **Is personal information transferred out of EEA, Switzerland or the UK?**

The EU and UK GDPRs contain specific requirements regarding the transfer of personal data collected in the EU or UK.

To determine whether specific requirements are needed, please confirm whether any personal data collected in the EU or UK is being transferred to a country outside the EU or UK.

Here is the EU official list of European Economic Area (EEA) countries (europa.eu)

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Yes

Justification

GSK US CPO Data Generation team

6.9 **Which country/ies is the personal information transferred to?**

Please select any and all countries that the personal information may be transferred to.

This could include:

- *where the personal information is sent to to be stored*
- *where other GSK departments are accessing the personal information from another country, for example in an off-shore operations centre*
- *where personal information is shared with a service provider who accesses or stores this in another country*

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

United States

Justification

None

6.10 **Which of the following sectors best applies to this activity?**

These are internal GSK definitions to help us decide whether an International Transfer Impact Assessment is required.

Please hover over each option below to obtain further information.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Pharma & life sciences service providers

Justification

None

6.11 **Does the third party subcontract the processing of GSK personal information to an organisation based outside UK, Switzerland, or EEA?**

Please indicate whether any third parties involved in this activity use any sub-processors to process our information on their behalf.

This includes anyone acting on behalf of the third party including sub-contractors or affiliates or third parties, or other organisations to which the third party may transfer the personal information.

If third parties are using a sub-processor, please detail who they are and where they are located, if possible. Please speak to Privacy Contact or Privacy Lead for further support.

Response

No

Justification

MyTomorrows is not using any subcontractors

6.12 **What type of data is exported?**

These are internal GSK definitions to help us decide whether an International Transfer Impact Assessment is required

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Research & Development (R&D) Data

Justification

None

6.13 **What suitable safeguards are applied to the international transfer?**

Many jurisdictions require safeguards to protect personal information that is transferred out of the jurisdiction it was collected in. Your privacy contact or lead can help you identify what safeguards are relied upon for this activity.

For personal information collected in the EEA, Switzerland or the UK a safeguard might not be required if the transferred is going to a country within the adequacy list. The list of countries that the European Commission has so far recognised as adequate can be found here.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Standard Data Protection Clauses adopted by the EU commission

Binding Corporate Rules

Justification

None

6.14 **Supplementary Measures**

Select the following measures that are implemented by the data importer and provide a justification for your selection(s).

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Pseudonymization

Full encryption of data in transit and at rest (key not accessible to data importer)

Justification

As part of the Study, the Centers will be responsible for removing all patient identifiable information and will ensure that the data is pseudonymized in an electronic capture (EDC) system: Castor EDC. Only participating Centers will have access to encryption key for patient identification. Pseudonymised data is stored on the secure and compliant cloud based EDC system, Castor EDC. Castor is ISO27001 (Information Security Management System) and ISO9001 (quality management system) certified. If downloaded from the system, it will be stored in an access controlled data management system on an external archive Oasis, not on any computers. Laptop computers are solely used in home offices and the myTomorrows office and will always be locked if unmanned. Oasis is a contracted qualified service provider. In Oasis Bridge (Oasis' software system) there is full traceability of the material, and retention timeframes are set and periodically reviewed for document destruction activities. The data transfer is done through GSK CSI Teams site. All GSK employees must comply to VQD-STD-000916 Privacy Standard.

7 Security

7.1 **What is the outcome of the Third Party Security Assessment?**

A Third Party Security Assessment (i.e., TPSA) is performed by the cybersecurity team on a third party and/or on its applications, systems and platforms, when GSK's cybersecurity criteria are met.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Reasonably Adequate

Justification

None

7.2 **Has a Risk and Compliance Assessment (R&CA) (previously known as a Smart Control Assessment) been completed and submitted?**

Risk and Compliance Assessment (R&CA) (previously known as a Smart Control Assessment) are defined to ensure that technology systems meet GSK and Regulatory requirements (e.g., audit trails, access management, electronic records and signatures, validation, privacy) and allow GSK to manage its main technology risks.

They must be conducted for all systems and maintained through the life of the system.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Yes

Justification

None

8 Transparency

8.1 **Have you or will you provide individuals with a privacy notice?**

Where a third party is used to provide the privacy notice, please describe how GSK evidence that the privacy information has been given to the individual. For example, if an agency / health care partner / intermediary provide privacy notice to individuals on behalf of GSK.

If multiple options apply, please provide further information in the justification box below.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

We rely on a third party to provide the individuals with a privacy notice

Justification

None

8.2 **Has the privacy notice been reviewed to ensure the processing covered?**

The privacy notice is public facing and can be found on our websites.

If the activity being assessed is not covered by the existing wording, then the privacy notice may need to be updated before the activity can start.

If a third party is being used to provide a privacy notice, this should be reviewed to confirm that it includes the required information.

If you require further assistance, please speak to a Privacy Contact or Privacy Leader.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Yes

Justification

None

9 Retention

9.1 **How long is the information held for?**

Select the applicable GSK Global Retention Schedule(s) for each type of data subjects (you selected data subject types in question 2.1). If none of the GRS applies to your processing activity, please identify and mention the relevant retention period(s) in the justification box below.

As an example: Employees: employee records (GRS056 - 7 years after employment ends) HCP: Healthcare Events Programme Records (GRS101 - <10 years).

If you are unsure, please access the GSK Global Records Retention Schedule.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

10 years

Justification

None

9.2 **When does the retention period start from (trigger)?**

This is the point from which the clock starts for deletion, this is often at the end of a relationship, closure of an account, the date a clinical trial ends.

For example, the period of retention for GSK employee personal information, only starts when an individual leaves employment. The trigger period, therefore, is when an employee ceases their employment with GSK.

Personal information will be kept for the length of the retention period from the trigger date, it will then be disposed of at the end of the retention period.

Response

The retention period starts from the end of the study (finalisation of the final study report).

9.4 **Is digital personal information automatically deleted and is hard copy personal information scheduled for deletion on a periodic basis?**

Where information is used digitally, is there a process that destroys information (or puts in beyond use) without human input?

Where information is stored physically, for example in archive, is there a process to ensure that the information is destroyed regularly?

If the answer to either is No, please select No as the answer and provide an explanation.

Response

Yes

Justification

GSK does not receive personal information, only pseudonymized data report. GSK archives pseudonymized data for 10 years.

9.5 **Can you prevent automatic and/or scheduled deletion from taking place?**

If we needed to, could automated deletion be paused or stopped? For example if we needed to keep information as part of a legal dispute, could it be kept longer than the original intended retention period?

Response

Yes

Justification

Yes we would be able to prevent deletion of data, if needed.

9.6 **How does GSK ensure personal information is managed in line with the retention period?**

This is particularly important where retention and deletion processes are not automated or where information is not stored in a structured system.

Please describe the processes or controls that will help us understand how long information is being held for an will ensure that it is deleted at the right time

Response

The used systems have the required features to manage records both in line with the Global Retention schedule and as required for litigation holds.

9.7 **Can GSK delete the personal information on request?**

In some countries individuals can ask for their information to be deleted, if we were asked to delete information by an individual, could their information be deleted? If information may not be deleted or there may be difficulties deleting it, please provide details.

If no is selected please provide a rationale in the justification box below.

Response

Yes

Justification

The data used for this activity is pseudonymized and cannot be attributed to identifiable individual without additional information held separately by the participating study site personnel. Consequently, we cannot determine whether a specific individual is included in the dataset. Should GSK receive a deletion request from an individual, it will be forwarded to the appropriate data holder (Center) for action.

9.8 **Please provide the GSK Global Retention Schedule (GRS) number(s).**

Please enter the relevant GRS numbers for the data elements collected for this processing activity. For more information on GRS numbers, you can consult the GSK Global Records Retention Schedule.

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

Retention of 10 years for both data stored by GSK and by the TP vendor from the conclusion of the study.
GRS040 for GSK (Supportive Regulatory Information - Key records relating to obtaining and maintaining product registrations but not submitted to an agency or 3rd party).
GRS050 for TP (CRO) (Contracts / Agreements - Documentation detailing the legally binding terms and conditions of agreements between the Company and other people / organisations).

Justification

None

10 Consultations

10.1 **Who has been consulted as part of the activity?**

It may be beneficial to seek opinion of others to fully consider risks and benefits. For example HR and/or Trade Union Representatives may be consulted for high risk change impacting GSK employees You can add links or upload output.

Response

Country Privacy Advisor for Italy; Asset lawyer

11 Supporting Information

11.1 **(Optional) Please provide links to any documentation that may support the assessment**

This is optional.

Examples of supporting documentation include data flow diagrams, system architecture diagrams, stakeholder consultation output, risk discussions/acceptance etc.

Response

Not answered

12 For Privacy Contact / Privacy Lead

12.1 **Is it necessary to consult with the Data Protection Authority?**

If a high risk has been identified and the risk cannot be mitigated, it may be necessary to consult with the Data Protection Authority

Response

No

Justification

No, the DPA has only to be notified with the publication of the PIA

12.2 **(Optional) Additional Comments**

Response

Not answered

13 Risks

13.2 **Based on the answers provided, there is a risk that individuals are not informed about how GSK use their information and their rights in relation to the information, or that the activity is unexpected.**

Questions answered that triggered risk:

Have you or will you provide individuals with a privacy notice? Answer: We are not required to provide individuals with a privacy notice for this activity.
or
Have you or will you provide individuals with a privacy notice? Answer: We rely on a third party to provide the individuals with a privacy notice.
or
Has the privacy notice been reviewed to ensure the processing is covered? Answer: No

Have you or will you put in place any actions to mitigate the risk? *Select Yes and use the justification box below to detail any mitigating actions taken. If No, use the justification box below to detail how this risk was accepted or closed.*

Response

Italy_Study 224207 retrospective use of data | Research & Development

Response

No

Justification

For non reachable patients, the Privacy notice will be published on a dedicated GSK web site.

13.15 **Are there any other risks that you have identified?**

If so, please detail them in the box below.

Response

Not applicable

Informativa sul trattamento dei dati personali

Studio 224207

Premessa

I Suoi dati, in particolare quelli personali e quelli sulla salute e soltanto nella misura in cui sono indispensabili in relazione allo scopo dello studio, verranno trattati nel rispetto del Regolamento Generale sulla Protezione dei Dati Personali EU 679/2016 (GDPR) e il Decreto legislativo n. 196/2003 così come modificato dal D.lgs. 101/2018 e ss.mm. I documenti relativi ai partecipanti saranno custoditi in luogo sicuro e non riporteranno i nominativi in chiaro, noto solo ai ricercatori, ma solo un codice identificativo.

Il Regolamento Generale sulla Protezione dei Dati Personali (GDPR) dell'Unione Europea stabilisce che GSK e i Centri, in qualità di titolari autonomi del trattamento dei dati, devono indicare le basi legali del trattamento delle informazioni personali (Articolo 6.1). Le basi giuridiche seguite da GSK sono di seguito riportate:

Tipo di informazioni personali	Base giuridica del GDPR
Informazioni sullo Studio (dati identificativi, dati sanitari) Origine etnica	Coerente con il legittimo interesse del titolare del trattamento ai sensi dell'Articolo 6.1 (f), e ai sensi dell'articolo 9.2 (g) e (j), perché il trattamento di categorie speciali di dati è necessario per la ricerca scientifica per motivi di interesse pubblico rilevante e sulla base del diritto dell'Unione o degli Stati membri, nonché ex art. 110 e 110bis del d.lgs. 196/2003.

Le Sue informazioni personali non saranno utilizzate per valutazioni eseguite mediante processi automatizzati senza coinvolgimento umano.

Perché verranno raccolti i dati codificati?

GSK utilizzerà i Suoi dati personali codificati per:

- Condurre e raggiungere lo scopo dello studio.
- Comprendere i risultati di questo studio.
- Progettare nuovi studi relativi al farmaco/vaccino in studio, alla malattia in studio e condizioni correlate.
- Pubblicare i risultati dello studio. Il Suo nome non apparirà in nessuna pubblicazione.

Come vengono protetti i Suoi dati personali? Cosa succede quando i dati vengono trasferiti?

Per proteggere i Suoi dati personali verranno adottate misure adeguate in accordo alle leggi applicabili in materia di protezione dei dati e di tutela della privacy.

I Suoi dati codificati (pseudonimizzati) potranno essere trasferiti in altri paesi a soggetti terzi che soddisfino requisiti di garanzia e che saranno contrattualmente vincolati alla protezione dei Suoi dati personali. In alcuni paesi le leggi sulla protezione dei dati potrebbero essere meno severe che in Italia. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, saranno adottate tutte le garanzie previste dall'articolo 46 del GDPR 679/2016 relative al trasferimento.

Maggiori dettagli sulle misure di tutela sono consultabili agli indirizzi:

- https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (Clausole contrattuali standard della Commissione europea per il trasferimento internazionale);
- https://ec.europa.eu/info/index_en
- https://www.gsk.com/en-gb/about-us/policies-codes-and-standards/binding-corporate-rules/ (GSK's Binding Corporate Rules)

Quali sono i Suoi diritti relativi ai Suoi dati?

Lei gode di alcuni diritti di cui riteniamo necessario informarLa. In alcune circostanze, alcuni Suoi diritti potrebbero essere limitati, ad esempio da requisiti legali per conservare una copia dei documenti di studio o per proteggere l'integrità scientifica di uno studio.

Lei ha il diritto:

- di conoscere con maggior dettaglio come vengono trattati i Suoi dati;
- una copia dei Suoi dati;
- di correggere le informazioni che Lei ritiene inesatte o incomplete;
- di richiedere la cancellazione dei Suoi dati;
- di chiedere l'invio dei Suoi dati ad un altro soggetto (ad esempio il Suo medico curante) per poterli riutilizzare.

Inoltre Lei potrà:

- opporsi al trattamento dei Suoi dati;
- sporgere reclamo all'autorità competente in caso di violazione dei Suoi diritti in materia di tutela di dati personali. In Italia l'autorità competente è il *Garante per la Protezione dei Dati Personali* (dati di contatto sul sito http://www.garanteprivacy.it);
- richiedere il risarcimento dei danni materiali o morali patiti in ragione di un trattamento illecito dei Suoi dati.

Per effettuare tali richieste, si consiglia di contattare prima la Sua regione di residenza. GSK non può rispondere a richieste pervenute direttamente da Lei, in quanto GSK non è in possesso dei dati identificativi dei pazienti e non è in grado di tracciare o isolare i singoli pazienti.

Per quanto tempo saranno utilizzati i Suoi dati?

I dati codificati saranno utilizzati esclusivamente per il periodo necessario allo svolgimento dello Studio, successivamente saranno cancellati trascorsi 10 anni dallo conclusione dello Studio.

Chi raccoglierà e utilizzerà i Suoi dati?

Il Titolare del Trattamento dei Dati raccoglie ed elabora i dati e stabilisce a quale scopo e come essi debbano essere elaborati. GSK e il Centro sono i Titolari autonomi del Trattamento dei Dati per questo Studio. Il Responsabile della Protezione dei Dati Personali (*Data Protection Officer*) di GSK può essere contattato all'indirizzo EU.DPO@gsk.com.

Per mantenere l'anonimato, La invitiamo in prima istanza a contattare il suo centro di riferimento. GSK non è in grado di rispondere a richieste ricevute direttamente in quanto non è in possesso dei dati identificativi dei partecipanti.

Ultimo aggiornamento 29/04/2026