onetrust

Assessment details

[redacted]

Name R&D - DPIA Global Clinical Development

Organization Clinical

[redacted]

Template PTC PIA/DPIA

Workflow Default assessment workflow

[redacted] 08/14/2025 11:40 AM

Date submitted 11/01/2024 02:56 PM

Last updated 08/14/2025 11:40 AM

Stage Completed

[redacted]

Status Active

[redacted]

Result Approved

[redacted]

Primary record id 5

Primary record name R&D - Global Clinical trials

[redacted]

Assessment questions

1 General

1.1 What activity are you assessing?

Response

R&D - Global Clinical trials | Clinical

[redacted]

1.2 Provide a description of the activity.

[redacted]

Response

R&D - Global Clinical trials | Clinical

Response

The types of research that fall within the scope of this DPIA are "Clinical trials" as defined by the Clinical Trial Directive (Directive 2001/20/EC) ("CTD" or the Directive") and as soon as it is in force, by the Clinical Trial Regulation (Regulation (EU) no. 536/2014 relating to clinical trials on medicinal products for human use and repealing Directive 2001/20/EC) (the "CTR" or the "Regulation"), including: - Interventional studies which trigger an intervention on the individual that is not justified by routine care; - Interventional studies that involve only minimal risks and constraints (e.g., low intervention trials); - Research requiring the examination of hereditary or acquired genetic features; - Biomedical research. Assets: Databases: Clinical Trial Databases are collectively defined as "CTBD" and include all Electronic Data Capture (EDC) for all study data e.g. safety vendor/system, central lab system, central imaging, etc. Sponsor's servers Information on the electronic systems and supporting assets listed above as well for all the processes, i.e. collection, retention, use, transfer, destruction that process the following types of personal data can be found in the in applicable agreements and/or list of electronic systems in the Study Specific Annex. Process: In principle Electronic data capture (EDC) system set-up for each trial is outsourced to a clinical vendor [redacted] either through a governance agreement or a separate agreement executed prior to the establishment of such governance agreement. Because the data management activities are outsourced to the CRO selected for the study, the CRO is responsible for the study data (defines EDC specifications, data validation specifications and takes care of data transfers agreements). The CRO obtains from the site coded patient level data. The study teams access the EDC system directly. The minimization principle is applied and the platform is accessed as required to ensure the sites are entering data on an ongoing basis. Coded patient level data is accessed through EDC. IT and Clinical QA assesses the clinical vendors prior to their appointment and before an agreement is executed with the vendor. As part of the assessment a detailed questionnaire is being answered.

[redacted]

1.3 What is the purpose of this activity?

Response

R&D - Global Clinical trials | Clinical

Response

Scientific research | Clinical Trials

Justification

PTC is a life sciences company that is developing therapies especially for rare diseases and acts as a sponsor of multiple global clinical trials. During the course of its clinical trials, certain processes remain consistent, regardless of the specific indications under investigation.

1.4 What is the primary business function that this activity support?

Response

R&D - Global Clinical trials | Clinical

Response

Clinical operations

Justification

Processing of personal data in this context mainly relates to individuals who are included in clinical research studies (hereinafter "trial participants"), and in particular in interventional studies involving human beings, for the purpose of performing the clinical research in the public interest, and for which the purpose of the research requires, prior to his/her inclusion in the research, the collection of the patient's informed consent, or that of his/her legal representatives.
Processing includes, but is not limited to, the sponsorship, conduct and management of such clinical research and the related clinical research data, with a view to enabling the collection, entry, validity and consistency checks and analysis of such data collected in the course of the research, within the framework of the clinical research protocol and the approved informed consent forms ("ICFs").
Processing relates also to the collection and processing of personal data relating to legal representatives of trial participants, as applicable, as well as and research professionals such as the study investigator or principal investigator and other research staff conducting the research within the framework of the clinical research protocol and the research objectives.
Processing relates also the collection and processing of personal data relating to research professionals for the purpose of implementing and performing the research, monitoring of the research professionals and compliance with the legal obligations of PTC as the sponsor of the trials, as well as processing relating to the management of human resources and training.
Finally, processing also relates to the collection and processing of personal data relating to employees, contractors and legal representatives of business partners, suppliers and vendors, providing services, under a contractual arrangement with PTC acting for and on behalf of PTC within the context of the clinical research activities.

1.5 Who are the key participants in this activity?

These are the groups who will participate in planning, overseeing and carrying out the processing activity.

You may also list the specific individuals involved.

Response

External Parties | IT | HCPs | CROs | R&D | Clinical trial sites | Third party vendors | Legal | Independent Committees

Justification

Sponsor
Sponsor is the data controller of the trial participants' coded data in order to conduct the study and exercises oversight of each of the vendors used in the context of the trial.

Sponsor directly contracts with the third-party vendors listed in the relevant Study Specific Annexes who are considered other data controllers or processors, depending on the respective services, roles and responsibilities, in connection with study data activities as noted in such Annexes.
Sub-processors should provide attestation or confirmation of GDPR compliance.
[redacted]
A list of sub-processors (if any) is included in the Study Specific Annexes.

Other processors and controllers in the conduct of the study include:
- **Clinical sites** (collect and store clinical data, personal medical/health records and other personal identifiable information). They shall be considered Independent Controllers; - Clinical sites (house clinical data collected, personal medical/health records and other personal identifiable information);
- **Health care professionals**
any member of the medical, dental, pharmacy and nursing professions (including physicians, psychiatrists, psychologist, pharmacists, investigators, academic consultants and their associated healthcare professionals such as physician assistants, advances nurse practitioners and nurses) and their support staff (such as site coordinators, administrative assistants, etc.), formulary decision makers and other individuals not employed by PTC who are in the position to influence the ordering, prescribing, purchase, use or recommendation of a PTC product.) conducting the study procedures. They shall be considered as Processors.
-Health care professionals, investigators as well as clinical research staff (i.e., study physicians, nurses, pharmacists, data coordinators, clinical research coordinators, etc.) conducting the study procedures.

- **Third-party vendors** (i.e., CROs, database providers, direct to patient services, central laboratories, etc.) access personal data only as required per the protocol. In principle they shall be considered Processors of the sponsor or of the clinical site, depending on the specific circumstances of the case.
- **Independent committees** (e.g., Ethics Committees (ECs), Investigational Review Boards (IRBs), Safety Data Monitoring Committees) act as Data Controllers within the framework of their particular mission and tasks.

1.6 Who is the owner of this business process?

[redacted]

Response

R&D - Global Clinical trials | Clinical

[redacted]

1.7 What is the projected go-live date?

If specific date is not known, please select the first day of the projected month.

[redacted]

1.8 What data is involved in the activity?

Please select the groups of individuals you are processing data about for this activity, and for each group, select the categories of data and individual data elements processed.

Response

Suppliers/3rd party Vendors

Employment information
- Job title role
- Office location
- Corporate credit or debit card numbers

Personal identification
- First name
- Full name
- Last name

Financial
- Bank account information

Contact information
- Phone numbers
- Contact details
- Personal email

Contractors

Personal identification

- Full name

Employment information

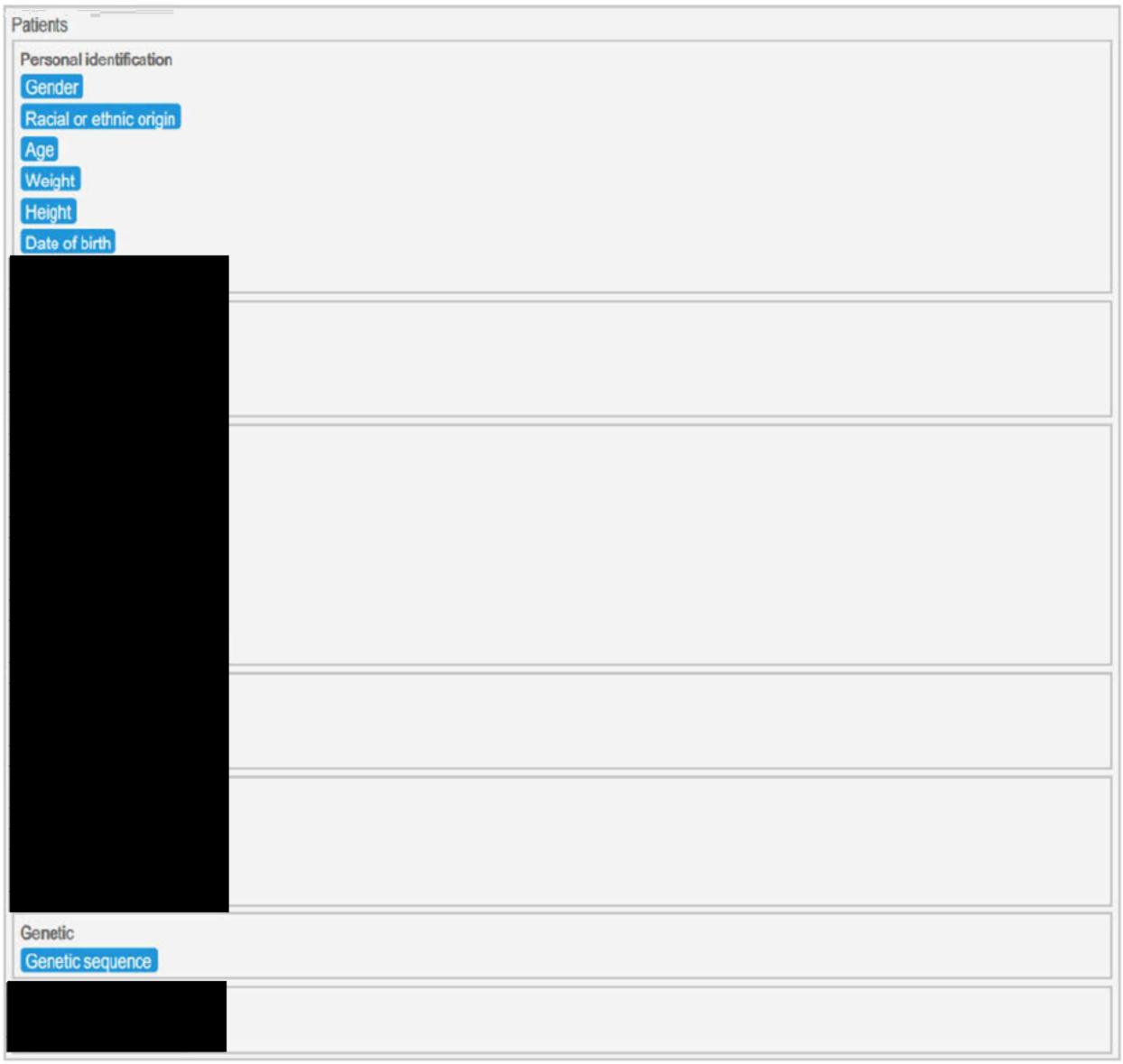
- Office location
- Job title role
- Company entity

Contact information

- Personal email
- Contact details
- Phone numbers

Financial

- Bank account number
- Routing number
- Bank account information


Patients
Personal identification
Gender
Racial or ethnic origin
Age
Weight
Height
Date of birth
[redacted]
Genetic
Genetic sequence
[redacted]

Healthcare Providers [HCP]

Financial
- Bank account information
- Bank account number
- Routing number
- Credit card number

Contact information
- Personal email
- Phone numbers
- Contact details

Personal identification
- Full name
- Last name
- First name

Education & Skills
- Academic transcripts
- Education and training history
- Educational degrees

Employment information
- Business unit division
- Personnel number
- Job title role
- Office location

Professional Experience & Affiliations
- Qualifications certifications
- Professional memberships

Caregivers

Contact information
- Contact details
- Emergency contact details
- Phone numbers
- Personal email

Personal identification
- Last name
- First name
- Full name
- Signature

[redacted]

Personal data relating to specific categories of individuals, are commonly collected and processed across all PTC sponsored interventional studies; These data are collected by the sites in a directly identifying format through the source documentation some of which is shared with the Sponsor in a coded (de-identified) format:

- Trial participants' personal data;
- Clinical site, vendor or sponsor's staff personal data

1.9 What operations will be performed on the data?

Please select all that apply. If you did not select any data elements in the previous question, select "Not Applicable."

[redacted]

Response

Storing | Organizing | Using | Erasing | Disclosing | Collecting

Justification

The investigator must ensure that the patients' confidentiality will be maintained. On the documents submitted to the sponsor or designees, patients should not be identified by their names, but by the assigned patient number. [redacted]

The investigator must treat all information related to the study as confidential, whose use is for conducting the study. The sponsor must approve any transfer of data not directly required by the study.
All personal data collected are stored in Clinical Trial Database ("CTDB") throughout the duration of the study.
Sponsor maintains organizational and security measures to safeguard Personal Data from loss, misuse, unauthorized access, disclosure, alteration or destruction.

Sponsor will ensure there is an existence of safeguards in place with the CTDB such as encryption and pseudonymization. Sponsor will ensure, taking into account the factual circumstances of the transfer in question, that an adequate or essentially equivalent level of protection is afforded to the data being transferred.

CRO will ensure those same safeguards are in place for any vendor that is subcontracted.
Sponsor will conduct ongoing reviews of any security measures. Only authorized users will be able to access, alter, disclose or destroy data and will remain within their scope of authority and delegation.
To protect unlawful cross-border transfers of personal data, sponsor requires its vendors to establish and maintain appropriate safeguards to protect the personal data that is being transferred to follow all global and local requirements.
All documentation relating to the study is retained for the period required by applicable local law.
The timeline for archiving data or deleting data follows national and regional laws and regulations.

1.10 Where are the individuals located?

Response

R&D - Global Clinical trials | Clinical

Response

United States | Central America/Caribbean/Mexico | Middle East | Asia-Pacific | Europe (Non EEA) | California | Canada | South America | Europe (United Kingdom) | Africa | Europe (EEA)

Justification

None

1.11 What is the number of individuals whose data are expected to be processed as part of this activity/

Response

R&D - Global Clinical trials | Clinical

Response

1000-10,000

[redacted]

1.12 Does the activity involve the processing of data of children under age 13? Please explain and specify the possible age range.

Response

Yes

[redacted]

[redacted]

1.13 Does the activity involve the processing of data that could reveal any of the following?

- *racial or ethnic origin;*
- *political opinions;*
- *membership of a political association;*
- *religious beliefs or affiliations;*
- *philosophical beliefs;*
- *membership of a professional or trade association;*
- *membership of a trade union;*
- *sexual preferences or practices;*
- *criminal record;*
- *health data;*
- *genetic data; OR*
- *biometric data.*

Response

Yes

Justification

Clinical trials might include sensitive data, mainly health, genetic, biometric, and racial or ethnic origin data

[redacted]

1.14 Do you intend to anonymize or pseudonymize any of the data? Please specify and explain.

Response

Pseudonymize

Justification

Pseudonymization

A trial participant's personal data are pseudonymized (assigned a code) by study sites before transferring to sponsor or its contractors. Specifically, a unique subject ID is assigned to each trial participant.
Sponsor and its processors do not have access to re-identify the data.
Personal data is stored in the CTDB as this is needed to analyze safety and efficacy data. When the personal data is included in a report outside the sponsor (ie. contracted vendor), this information is masked such that those receiving the data are unable to identify the patient.

Minimizing the amount of personal data collected

The intent of sponsor's processes is to collect minimal personal data needed to conduct job tasks and/or functions under the defined protocol and company and/or vendor SOPs.

1.15 Are the data collected directly from the individual, from third parties, or both?

Response

R&D - Global Clinical trials | Clinical

Response

Directly from individuals | Asset or vendor

[redacted]

In principle Electronic data capture (EDC) system set-up for each trial is outsourced to a clinical vendo[redacted] either through a governance agreement or a separate agreement executed prior to the establishment of such governance agreement.
Because the data management activities are outsourced to the CRO selected for the study, the CRO is responsible for the study data (defines EDC specifications, data validation specifications and takes care of data transfers agreements). The CRO obtains from the site coded patient level data.
The study teams access the EDC system directly. The minimization principle is applied and the platform is accessed as required to ensure the sites are entering data on an ongoing basis. Coded patient level data is accessed through EDC.
IT and Clinical QA assesses the clinical vendors prior to their appointment and before an agreement is executed with the vendor. As part of the assessment a detailed questionnaire is being answered.

10. How do you get this information ?
- Patients' data: from the Principal Investigator of the study which has pseudonymized/coded the patients' data
- HCPs data: from the HCPs directly or from the institution/clinical site
- Clinical vendors' staff data: from the clinical vendor directly

1.16 What assets does the data come from?

[redacted]

Response

Clinical Trial Databases | PTC Therapeutics, Inc. [redacted] | Site sponsor servers | PTC Therapeutics, Inc. [redacted]

[redacted]

1.17 What assets are used to store and process the data for this activity?

In other words, after the data is obtained, where will it spend most of its time? Will it stay put, or will it go somewhere else? In terms of flow, this would be somewhere in the middle.

An 'asset' is something that supports information-related activities. Assets could include software systems, applications, databases, or even file cabinets.

Response

Site sponsor servers | PTC Therapeutics, Inc. | [redacted]

Clinical Trial Databases | PTC Therapeutics, Inc. | [redacted]

Secured portal (clinical trials) | PTC Therapeutics, Inc. | [redacted]

[redacted]

1.18 What assets is the data transferred to?

In other words, does the data go anywhere after being in the storage assets? In terms of data flow, this would be somewhere near the end.

An 'asset' is something that supports information-related activities. Assets could include software systems, applications, databases, or even file cabinets.

Response

Secured portal (clinical trials) | PTC Therapeutics, Inc. | [redacted]

1.19 Who will have access to and/or use the data?

Response

R&D - Global Clinical trials | Clinical

Response

HCPs | External agencies | Independent Committees | Internal employees on need to know basis | Site Sponsors | Public Authorities/Government Bodies | B2B customers | CROs | Service providers | Internal auditors | Clinical Trial Sites | External auditors

Justification

All clinical study data are transferred via a secured portal or external media eg, During study conduct, data are transferred via secured portals. At study completion, study records are transferred to PTC by CRO via a secured portal, direct transfer (system to system), or password-protected media and the password is sent separately by email.

[redacted]

Clinical study data are transferred during study conduct and after study completion. Subject identifiers are pseudonymized, subject data is captured in case report forms with sensitive data eg, reaction to treatment, adverse events. HCPs data are captured in CVs and Medical Licenses.

How is the data transferred? All clinical study data are transferred via a secured portal or external media eg, During study conduct, data are transferred via secured portals. At study completion, study records are transferred to PTC by CRO via a secured portal, direct transfer (system to system), or password-protected media and the password is sent separately by email.

[redacted]

Databases:
Clinical Trial Databases are collectively defined as "CTBD" and include all Electronic Data Capture (EDC) for all study data

[redacted]

[redacted]

1.20 Where are these parties located?

Response

R&D - Global Clinical trials | Clinical

Response

Global

[redacted]

2 Privacy Principles

2.1 What steps have you taken to ensure that the data are processed fairly?

Please choose from the following, and/or add your own.

Response

Privacy tools, settings and functionalities are clear, conspicuous, easy to find, and user-friendly

[redacted]

2.2 What steps have you taken to ensure that the data are processed in a transparent manner?

Please choose from the following, and/or add your own.

Response

Each clinical trial subject receives ICF

Notice to HCPs is provided

Users are provided with the ability to report problems/concerns

Browser add-ons to assist with privacy are provided to users

Users are made aware of who is collecting/using their data

[redacted]

2.3 What steps have you taken to ensure that the data are collected and used only for specified, explicit and legitimate purposes?

[redacted]

[redacted] | The specific purpose for every data element is documented | The purpose of every data element is identified prior to collection

Justification

Considering that in many cases the trials are conducted globally on a multicenter level and that legal justifications (or "legal basis") for the collection and processing of personal data vary based on local legislation and its interpretation by relevant national (and regional) authorities, legal basis will vary depending on the location of the sites in which the trial is being conducted. For Europe (EEA, Switzerland, UK) specific provisions of GDPR or of the CTR or simare referred to for each legal ground for completeness.

The basis for making the processing lawful forsubject data includes one or more of the below elements:

- Compliance with global regulatory and local legal law requirements and obligations resulting from the clinical trial laws;

- Legitimate interest of the sponsor in conducting the study;

- Consent: Consent of the subjects is collected through the Informed Consent Form. The clinical research site staff obtains the patient's informed consent prior to sending PTC the subject's personal information. The investigator maintains a record of this consent and notifies PTC that it has been obtained.

-Basis for processing sensitive data for reasons of public health interest (e.g. ensuring high standards of quality and safety of our product).

[redacted]

2.4 What steps have you taken to ensure that data are not further processed in a manner that is incompatible with those purposes?

[redacted]

Processing, utilisation and transfer rights are restricted

Company policies are in place to minimise our exposure to hackers

Purpose specific pseudonyms, anonymisation services and/or anonymous credentials are used

Separation exists between organisations and departments

[redacted]

2.5 What steps have you taken to ensure that the data are limited to what is necessary for the purpose of this activity?

[redacted]

Data to be transferred is limited to that which is minimally necessary to achieve the purpose of the transfer

[redacted]

When the Protocol is prepared the categories of data to be collected are determined having regard to the patient privacy protection and ensuring that the sponsor only receives what is necessary to perform a valid analysis and not more.

2.6 What steps have you taken to ensure that the data are relevant to the purpose of this activity, accurate and kept up-to-date?

[redacted]

All data are regularly monitored and quality checks are implemented along with source document verification according to the Clinical Monitoring and Data Management plans to ensure reliability and robustness along with ensuring the contract between the vendor and sponsor is maintained.
Data collected will be maintained both by system/technical controls, as well as by defined process controls.

[redacted]

2.7 What steps have you taken to ensure that data are kept in a form that allows identification of individuals for no longer than is necessary for the purposes for which they are processed?

[redacted]

Response

Data inventory review and deletion processes are in place

[redacted]

2.8 Describe the data retention time limits.
How long will you keep the data involved in the activity?

[redacted]Clinical trials | Clinical

Response

All documentation relating to the study should be retained for the period required by applicable local law (e.g. Canadian regulation requires 25 years; EU regulation requires 25 years; US regulation requires sponsors to retain study documents for a minimum of 2 years after a product's last indication is approved or 2 years after a product is discontinued from development). If it becomes necessary for the sponsor, the sponsor's designee, applicable IRB/IEC, or applicable regulatory authorities to review or audit any documentation relating to the study, the investigator must permit access to all source documents/data.

[redacted]

3 Scope [Privacy/Legal]

3.1 Which of the following laws are applicable to this activity?
If you are unsure, consult with the approver of this assessment before continuing.

Response

Switzerland Federal Act on Data Protection 2020 (Revised) | Brazil General Data Protection Law | EU General Data Protection Regulation | Australia Privacy Act | Japan Act on the Protection of Personal Information | [redacted]

[redacted]

4 Legal Basis

4.1 What legal bases are you relying on for this activity?
You may provide additional information in the notes field below.

If you are unsure of the answer to this question, please select "not sure" and explain.

Response

Contract Performance | Consent | Legal Obligation | *Research [BRAZIL ONLY]

[redacted]

Page 17 Omitted Below

[redacted]

4.18 Does the request for consent have ALL of the following attributes?

1. *It is clearly distinguishable from other matters;*
2. *It is presented in an intelligible and easily accessible form;AND*
3. *It uses clear and plain language.*

Response

Yes

[redacted]

4.19 Does the consent have ALL of the following attributes?

1. *It is **freely given**—i.e., the individual has real choice and control over their decision;*
2. *It is **specific**—i.e., it is tied to a specific purpose and unbundled from other terms and conditions;*
3. *It is **informed**—i.e., information is provided to the individual to enable an informed decision);**AND***
4. *It is **unambiguous**—i.e., there is a statement or clear affirmative act signifying consent.*

Response

Yes

[redacted]

4.20 Is evidence of consent retained to demonstrate what each individual has consented to, what they were told, and when and how they consented?
This might include keeping records of:

- *consent statements received;*
- *the consent workflow at the time of consent;*
- *the information that was presented to the individual at the time of consent.*

Response

Yes

Justification

Yes clinical sites keep the executed consents on file [redacted]

4.21 Is there a way for individuals to withdraw their consent in a way that is as easy as it was to give it?
The process of withdrawing consent must be no more burdensome than the act of giving consent.

For example, if consent is obtained via electronic means through a mouse-click, swipe or keystroke, it must be equally as easy to withdraw that consent.

Response

Yes

Justification

this is specified in the different relevant parts of the ICF [redacted]

4.22 Is parental or legal guardian consent obtained before collecting the data of children?

[redacted]

Response

Yes

[redacted]

4.24 Is parental or legal guardian consent obtained before collecting the data of children under age 16?

Response

Yes

[redacted]

4.33 Which of the following allows to you process the sensitive data?

The processing of this type of data is prohibited, unless one of the following applies.

[redacted]

Response

Archiving, research or statistical purposes

[redacted]

[redacted]

[redacted]

5 Data Transfers

5.1 Does this activity involve the transfer of data to your affiliates, subsidiaries or parent entities?

Response

Yes

[redacted]

5.2 Does this activity involve the transfer of data to any external third parties?

Response

Yes

Justification

Appropriate transfer controls have been put in place.

In EU, Switzerland, UK, Brazil and other non EU privacy legislations, as applicable, the laws mandate specific legal mechanisms to send data outside of the original territory where it was collected from the data subjects.

[redacted]

Transfer between respectively (i) clinical sites or clinical vendors and (ii) PTC rely on the legal mechanisms foreseen under GDPR. PTC also follows its Global Privacy Policy. Each vendor contracted is assessed to ensure it abides by similar safeguards to protect personal identifiable information.
Personal data will be transferred pursuant to adequacy decisions (art. 45 GDPR) or any other adequate data transfer mechanism (art. 46 GDPR) including the adoption of specific contracts (notably the EU Standard Contractual Clauses (Controller to Controller) between sites and PTC). In adopting the appropriate data transfer mechanism as specified above and/or any supplementary measures, as required by applicable data protection laws and regulations, PTC will ensure, taking into account the factual circumstances of the transfer in question, that an adequate or essentially equivalent level of protection is afforded to the data being transferred through the conduct of transfer impact assessments.

[redacted]

[redacted]

Page 22 & 23 Omitted Below

[redacted]

5.6 Will any data be transferred out of the European Union (EU) / European Economic Area (EEA)?
Please list the recipient countries in the text box below. This includes all countries where the data will be accessed or shared.

The EU includes:

- *Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden*

The EEA includes:

- *All EU countries plus Iceland, Liechtenstein and Norway.*

Response
Yes

[redacted]

5.7 Which of the following legal mechanism(s) are in place for the cross-border transfer of personal data out of the EU/EEA?
Click here for the list of countries that have received an adequacy decision from the European Commission.

Response

R&D - Global Clinical trials | Clinical

[redacted]

legal transfer mechanisms vary depending on the countries and the relationship considerd (ie site/sponsor or sponsor/patient etc)

6 Privacy Rights

6.1 Is notice of the processing activity provided to individuals at or before the point of collection of their data? Please explain.
Consider all forms of notice—e.g., via website, mobile application, email, paper, physical signage, recorded audio, oral, etc.

Response
Yes

[redacted]

6.2 Is there a way to obtain detailed information about the processing of a specific individual's data? Please explain.

Response

Yes

Justification

Patients
Sponsor collects data for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Processing purposes are specified and explicit in the study protocol, the informed consent(s) and CTAs and follow all applicable legal requirements per global and local guidelines.

[redacted]

- Obligations and scope of services of the respective processors are clearly identified and governed by the applicable Master Service Agreement and more specifically within the vendor's scope of work.

- Processing lasts for the duration of the study.

- All processing activities are governed by a data processing agreement.
For EU, each processing contract sets out all of the aspects stipulated in Art. 28 of the GDPR: duration, scope, purpose, documented processing instructions, prior authorization where a processor is engaged, provision of any documentation providing evidence of compliance with the GDPR, prompt notification of any data breach, etc.

Clinical trial's ICF(s). The ICF describes and explains the processing that will be performed on the patient's personal data in the event he/she decides to voluntarily participate in the study. The ICF contains easy-to-understand terms [redacted]

Investigators and clinical staff

The sponsor has prepared a privacy notice that is part of the template CTA and should be distributed by the site to explain the purposes of the collection and use of the data.

Vendors' staff data

Appropriate language is included in the vendor agreements to this effect.

6.3 Is there a way to confirm whether a specific individual's data is being processed, and provide them access to that data? Please explain.

Response

Yes

Justification

[redacted]

- All personal data controlled at site by the investigator is retrievable upon request by contacting the investigator.

- The sponsor only has access to coded personal data. Therefore although the sponsor can be contacted through the investigator, the sponsor will not be able to share much information nor answer many queries. The sponsor would in principle redirect the patient to the site if contacted to exercise access rights.

6.4 **Is there way to transmit a specific individual's data to them, or to another service provider, in a portable and readily useable format? Please explain.**

Response

Yes

Justification

[redacted]

Study patient's personal data:

[redacted] Each study patient can exercise their personal data rights by contacting the study site's personnel or CRO's data privacy officer.

- [redacted]

- All personal data controlled at site by the investigator is retrievable upon request by contacting the investigator.

- The sponsor only has access to coded personal data. Therefore although the sponsor can be contacted through the investigator, the sponsor will not be able to share much information nor answer many queries. The sponsor may redirect the trial participants to the clinical site.

6.5 **Is there a way to correct a specific individual's data if found to be incomplete, inaccurate or outdated? Please explain.**

Response

Yes

Justification

Data subjects can exercise their rights by contacting the site directly. If the data subject contacts sponsor's privacy officer, the data subject will be directed to study site personnel.
Contact details of the site are provided in the ICF.
Sites are obligated by contract to manage data subjects' questions [redacted]
If a patient requests their personal data, the site must comply with their request. When a site is contacted, the information provided will be documented in the patient's chart. The site will notify the vendor/sponsor.

All data are regularly monitored and quality checks are implemented along with source document verification according to the Clinical Monitoring and Data Management plans to ensure reliability and robustness along with ensuring the contract between the vendor and sponsor is maintained.

Data collected will be maintained both by system/technical controls, as well as by defined process controls.

Personal data of subjects are updated on a regular basis by clinical sites.

To ensure the highest data quality, there are data quality control measures implemented at the site including routine monitoring visits per the monitoring plan and remote monitoring.

Periodically, the sponsor or its authorized representatives audit clinical investigative centers and review core trial processes and documents to determine whether these activities were conducted, and data were recorded and accurately reported according to the protocol, GCP guidelines, and any applicable regulatory requirements.

[redacted]

6.6 **Is there a way to permanently stop the processing of a specific individual's data? Please explain.**

Response

Yes

Justification

withdrawal of consent or opposition depending on the legal grounds applicable to the specific relationship. Everything is detailed in the corresponding privacy notices

6.7 **Is there a way to temporarily restrict the processing of a specific individual's data? Please explain.**

Response

Yes

Justification

Temporary restricting of processing can occur only in cases of receiving request or withdraw of consent. Or in cases of lost to follow up or in cases of death.

6.8 Is there way to stop the transmission of a specific individual's data to third-parties? Please explain.

Response

Yes

Justification

In case when individual withdraws from the study, future data will not be transferred or processed for such an individual.

[redacted]

[redacted]

6.11 Have you checked to ensure that you WILL NOT take any action that could be perceived as discriminating against individuals that have exercised their privacy rights under the law?

[redacted]

Response

Yes

[redacted]

7 High Risk Activities

Page 29 Omitted Below

7.4 Does the activity involve sensitive data or data of a highly personal nature?

This includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals.

For example:

- *a general hospital keeping patients' medical records;*
- *a private investigator keeping offenders' details;*
- *electronic communications whose confidentiality should be protected;*
- *location data whose collection questions the freedom of movement;*
- *financial data that might be used for payment fraud;*
- *data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications*

DataGuidance:

- *EDPB/WP29 Guidelines on DPIAs and High Risk*
- *Guidance on the Data Protection Regulations 2021*

Response

Yes

Justification

Processing of personal data in this context mainly relates to individuals who are included in clinical research studies (hereinafter "trial participants"), and in particular in interventional studies involving human beings, for the purpose of performing the clinical research in the public interest, and for which the purpose of the research requires, prior to his/her inclusion in the research, the collection of the patient's informed consent, or that of his/her legal representatives.

[redacted]

[redacted] Page 31 & 32 Omitted Below

7.7 Could the activity involve data concerning any of the following vulnerable individuals? Select all that apply.

Under "other" you may include any case where a power imbalance exists in the relationship between the individual and the organisation.

You may provide additional information in the notes field below. If you are unsure of the answer to this question, please select "not sure" as your response and include any relevant information in the notes field below.

DataGuidance:

- *EDPB/WP29 Guidelines on DPIAs and High Risk*
- *Guidance on the Data Protection Regulations 2021*

Response

[redacted] Healthcare patients Elderly Children

Justification

Clinical trial subjects, minors to adults

[redacted]

[redacted]

[redacted]

7.15 Does the activity involve any of the following? Please explain.

Response

Providing personal information abroad

Entrusting personal information handling, providing personal information to other personal information handlers, or disclosing personal information

[redacted]

[redacted]

8 Necessity, Benefits and Harms

8.1 **How necessary is this activity in relation to the purpose? Please explain.**
Consider whether there might be a less privacy-invasive way of achieving the same purpose.

Response
Critical

Justification
It is legal obligation to collect meaningful patient data to be able to conduct a trial

8.2 **What are the potential benefits that could occur as a result of this activity? Please explain.**

Response
Scientific research

Justification
Foster scientific research, understand more about a disease or a condition, save lives

8.3 **Who will receive the benefits of this activity?**

Response
Society | Individuals | Our organization

[redacted]

Page 36, 37 & 38 Omitted Below

[redacted]

10 Additional Information

10.1 You're done!

Please provide any additional information here.

Page 40 & 41 Omitted Below

onetrust

Assessment details

ID 165

Name Milano Site Clariphy Study

Organization PTC Therapeutics, Inc.

Description PTC declares: publishing an extract of the DPIA on your institutional website containing essential information on the processing, the purposes pursued, the categories of data processed, the individuals involved, and the safeguards adopted; providing advance notification of the research program to the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali), pursuant to Article 110, paragraph 1, of the Privacy Code; providing the Authority with all the documentation necessary for the evaluation of the research program, including the complete DPIA; awaiting the Authority's ruling before proceeding with data processing without consent, if requested."

[redacted]

Respondent [redacted] Fernando Cortes

Template Clinical Annex Template v.3 (Based on OnePIA (Full) - 7.2.2) (Copy)

Workflow Default assessment workflow

[redacted]

Date created 05/19/2026 03:28 PM

[redacted]

[redacted]

Primary record id 5

Primary record name R&D - Global Clinical trials

Template version 3

[redacted] co[redacted]

[redacted]

[redacted]s

onetrust

Submission Progress (%) 100

Study specific Annex_ ITALY PKU_2026

Assessment questions

1 General Details of the Study

1.1 What activity are you assessing?

Response

R&D - Global Clinical trials | Clinical

[redacted]

1.2 Point of Contact for the Study

Response

R&D - Global Clinical trials | Clinical

[redacted]

DPIA questions: dataprivacy@ptcbio.com
subject line: PKU-2025-01 IT_Milan

1.3 Description

Response

R&D - Global Clinical trials | Clinical

Response

[redacted]an observational retrospective cross-sectional multicentric study based on hospital clinical records aiming at characterizing patient populations with PKU and their therapeutic management in 8 Italian centres. It is to be performed by using an electronic data collection form adapted for both adult and pediatric patients. Consult protocol (Annex M3) for details. [redacted] PIs will pseudonymize patient data according to a coding system only accessible to them. Access to the eForm will be provided to PIs through a link in the welcoming kick off mail [redacted] The mail and link will be shared with the principal investigators and the collaborating researchers appointed per centre. [redacted] PTC will only receive statistical analyses performed [redacted] as described in the approved protocol. The overall project has been approved by Bari's Ethics committee as the reference centre. [redacted]

[redacted]

1.4 Aims and Objectives of the Study

Response

Characterizing patient populations with PKU and their therapeutic management in 8 Italian centres.

1.5 Phase of Clinical Trial

Response

Observational Study

[redacted]

1.6 Has the Protocol been approved by authorizing bodies/ethics committees?

Response

Yes, the overall project has been approved by Bari's Ethics committee as the reference centre.

1.7 Protocol Code Number

Response
PKU-2025-01

[redacted]

1.9 Study Status

Response
Not yet recruiting

[redacted]

1.10 Start Date

Response
08/23/2026

1.11 End Date

Response
01/01/2027

1.12 Where are the individuals located?

Response

R&D - Global Clinical trials | Clinical

Response
Europe (EEA)

Justification

[redacted]

-Ospedale San Paolo-Asst-Santipaolocarlo (Milano)

[redacted]

1.13 What is the number of individuals whose data are expected to be processed as part of this activity?

Response

R&D - Global Clinical trials | Clinical

Response
0-1000

[redacted]

1.14 Is this a multi-site study?

Response

Yes

[redacted]

1.15 Does the activity involve the processing of data of children or minors? Please explain and specify the possible age range.

Response

Yes

[redacted]

1.16 Are there any study specific requirements at the national level?

Response

Amended Italian Privacy Code (2024) Article 110, impacting Medical, Biometrical, and Epiddemiological Reaserch paragraph 1, Authorization No. 9/2016 from the Privacy Authority [redacted]

2 Processor Information

[redacted]

2.2 Location

[redacted]

Response

Italy

Justification

None

2.3 Description

[redacted]

Response

Contacting Purposes, Scientific Support

Justification

None

2.4 Where are these parties located?

Response

R&D - Global Clinical trials | Clinical

Response

Italy

Justification

None

2.5 Do processors have access to patient identifiable data?

Response

No

Justification

Pseudonymized Data Only

2.6 Processor Assets

[redacted]

2.7 Hosting location

Response

[redacted]

Response

Italy

Justification

None

2.8 Other than the named processors and controllers, will the data be shared with anyone else or another third party?

Response

Yes

[redacted]

2.9 In which country will the data analysis be performed?

Response

Italy

[redacted]

2.11 How long will the data be retained after the analysis?

Response

he material generated during the study (final report, data analysis) will be stored at the Sponsor's offices for at least five years after the end of the study or for a longer period if required by other applicable regulations.

Individual patient data will not be retained.

2.12 Purpose of data collection

[redacted]

Response

Conducting observational st

Justification

None

3 Sub-Processor Information

3.1 Sub-Processors

[redacted]

will obtain pseudonymized data only on the specific set of variables described in the protocol (annex M3), promoter (PTC therapeutics) will obtain analyzed data only.

3.2 In which countries are these Sub-Processors located?

Response

Italy

3.3 For each of the vendors, in which country will the data be stored?

Response

Italy

3.4 Does Sub-Processors have access to patient identifiable data?

Response

No

4 Scope [Privacy/Legal]

4.1 Which of the following laws are applicable to this activity?

Response

Italy Personal Data Protection Code | EU General Data Protection Regulation

Justification

pursuant to amended Italian Privacy Code (2024) Article 110, impacting Medical, Biometrical, and Epiddemiological Reaserch paragraph 1, Authorization No. 9/2016 from the Privacy Authority. T[redacted]

5 Data Transfers

5.1 Does this activity involve the transfer of data to your affiliates, subsidiaries or parent entities?

Response

Yes

[redacted]

5.2 Does this activity involve the transfer of data to any external third parties?

Response

Yes

[redacted]

5.3 Will data be transferred across international borders? Please explain.

Response

Yes

Justification

Systems are Global

5.4 Will any data be transferred out of the European Union (EU) / European Economic Area (EEA)?

Response

Yes

Justification

Yes, PTC is a Global Company

5.5 Are there any other transfers in the context of clinical trials, besides what is included in the framework for the EU-US transfers attached? If unsure, please Contact the Privacy Office.

Response

No

[redacted]

5.7 Cross Border-Transfer Mechanism(s)

Response

R&D - Global Clinical trials | Clinical

Response

Yes

[redacted]

6 High Risk Activities

6.1 Does the activity involve new, or innovative uses of, technological or organisational solutions?

Response

No

[redacted]

6.2 Does the activity involve the sale of personal data?

Response

No

[redacted]

6.3 Would you like to answer additional questions about benefits and harms presented by the activity?

Response

Yes

Justification

There will be no benefit for individuals but for the whole community of PKU patients and treating clinicians

7 Controls

7.1 What controls have already been implemented to support this activity and mitigate risk?

Response

R&D - Global Clinical trials | Clinical

EU General Data Protection Regulation (GDPR)

- Art. 5(1)(c) : Data minimisation
- Art. 49(1)(b) : Cross-border transfer - derogations - contract with data subject
- Art. 46(2)(a) : Cross-border transfer - international law
- Art. 14 : Notice - data not obtained from data subject
- Art. 12 : Transparency and facilitation of data subject rights
- Art. 6(1)(e) : Legal basis - public interest
- Art. 11 : Processing which does not require identification
- Art. 49(1)(f) : Cross-border transfer - derogations - vital interests
- Art. 9(b) : Special categories - legal rights
- Art. 36 : DPIA prior consultation
- Art. 28(1) : Processor - sufficient guarantees
- Art. 13 : Notice - data obtained from data subject
- Art. 9(g) : Special categories - substantial public inerest
- Art. 28(5) : Processor - code of conduct or approved certification
- Art. 5(1)(f) : Integrity and confidentiality
- Art. 6(1)(c) : Legal basis - legal obligation
- Art. 18 : Right to restriction
- Art. 26 : Joint controller arrangement
- Art. 5(1)(e) : Storage limitation
- Art. 35 : Data protection impact assessment
- Art. 21 : Right to object
- Art. 49(1)(e) : Cross-border transfer - derogations - legal claims

- Art. 46(2)(e) : Cross-border transfer - Approved code of conduct
- Art. 9(a) : Special categories - explicit consent
- Art. 32 : Security of processing
- Art. 28(3) : Processor - contract
- Art. 5(1)(a) : Lawfulness, fairness and transparency
- Art. 46(3) : Cross-border transfer - supervisory authority authorization
- Art. 16 : Right to rectification
- Art. 24(1) : Technical and organisational measures
- Art. 9(i) : Special categories - public health interests
- Art. 27 : EU representative
- Art. 46(2)(d) : Cross-border transfer - standard data protection clauses adopted by supervisory authority and approved by EU Commission
- Art. 34 : Breach notification - data subject
- Art. 24(2) : Data protection policies
- Art. 6(1)(d) : Legal basis - vital interests
- Art. 28(2) : Sub-processor - written authorisation
- Art. 45 : Cross-border transfer - adequacy
- Art. 30 : Records of processing activities
- Art. 9(c) : Special categories - vital interests
- Art. 37 : Data protection officer
- Art. 33(2) : Breach notification - controller
- Art. 49(1)(a) : Cross-border transfer - derogations - explicit consent
- Art. 46(2)(c) : Cross-border transfer - Standard data protection clauses adopted by Commission
- Art. 5(1)(b) : Purpose limitation
- Art. 8 : Parental consent
- Art. 24(3) : Approved code of conduct or certification
- Art. 15 : Right of access
- Art. 49(1)(c) : Cross-border transfer - derogations - contract with third-party
- Art. 28(4) : Sub-processor - contract
- Art. 33(1) : Breach notification - supervisory authority
- Art. 17 : Right to erasure
- Art. 6(1)(a) : Legal basis - consent
- Art. 9(h) : Special categories - health or social care
- Art. 20 : Right to data portability
- Art. 6(1)(f) : Legal basis - legitimate interests
- Art. 9(j) : Special categories - archiving, research or statistical purposes
- Art. 25 : Data protection by design and by default

Art. 22 : Right to not be subject to automated decisions
Art. 31 : Cooperation with supervisory authority
Art. 19 : Third-party notification (rectification or erasure)
Art. 9(e) : Special categories - data made public by data subject
Art. 5(1)(d) : Accuracy
Art. 49(1)(g) : Cross-border transfer - derogations - public register
Art. 5(2) : Accountability
Art. 49(1)(d) : Cross-border transfer - derogations - public interest
Art. 29 : Processing instructions
Art. 6(1)(b) : Legal basis - contract
Art. 49(1) subpara. 2 : Cross-border transfer - derogations - suitable safeguards

7.2 Are there any additional controls that you would recommend for implementation?

[redacted]

8 Additional Control Questions

8.1 Please explain the arrangements to anonymize, archive or destroy personal data and/or samples once the health research has been completed.

Response

In the event of the termination of the Agreement in part or in whole, Service Provider shall, within fifteen (15) days of the request date, send to PTC all Personal Data held by Service Provider on behalf of PTC, together with all copies in any media of such data. If PTC requests, in a written form, to destroy the same, Service Provider will comply, unless Service Provider is under legal obligation to retain such data or a part thereof, in which case Service Provider will inform PTC immediately.
Once the study is published, the material generated during the study (final report, data analysis) [redacted]

[redacted]

8.3 Are measures in place to deny unauthorized persons access to processing equipment used for processing? Please explain.

Response

Yes

[redacted]

8.4 Are measures in place to prevent the unauthorized reading, copying, modification or erasure of data media?

Response

Yes

[redacted]

8.5 Are measures in place to prevent the unauthorized input of personal data and the unauthorized inspection, modification or deletion of stored personal data ('storage control')? Please explain.

Response

Yes

Justification

VIII. Physical data storage is in locked area, with entry for authorized personnel only.
V. Users processing sensitive data are authenticated and authorized with a strong password policy

[redacted]

8.7 Are measures in place to ensure that persons authorized to use an automated processing system have access only to the personal data covered by their access authorization? Please explain.

Response

Yes

Justification

1. DATA INTEGRITY
In order to ensure that integrity of any data stored, received, controlled or otherwise is maintained, the following are established:
- A process defining role based access management rules;
- A process for authentication of the authorized personnel;
- Utilization of user codes (passwords);

[redacted]

[redacted]

[redacted] Are measures in place to ensure that the confidentiality and integrity of personal data are protected during transfers of personal data or during transport of data media?

Response

Yes

Justification

Data is protected during transit using HTTPS encryption.
PTC Confidential data is encrypted in accordance with minimum baseline encryption standards while in transit and at rest.

8.11 Are measures in place to ensure that installed systems may, in the case of interruption, be restored? Please explain.

Response

Yes

Justification

Business Continuity Planning is established to restore availability and access to critical services by all staff ..

8.12 Are measures in place to ensure that all system functions perform and that the appearance of faults in the functions is reported? Please explain.

Response

Yes

Justification

Documented policies, procedures, and processes are checked for validity and updated on an annual basis unless an event that directly conflicts said documents, at which time they will be updated immediately. Technical, administrative, and operational procedures are in place to provide assurance that all products and processes are operating as intended.

8.13 Are measures in place to ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system? Please explain.

Response

Yes

Justification

Documented policies, procedures, and processes are checked for validity and updated on an annual basis unless an event that directly conflicts said documents, at which time they will be updated immediately. Technical, administrative, and operational procedures are in place to provide assurance that all products and processes are operating as intended.

8.14 Are measures in place to ensure that personal data processed on behalf of the controller can only be processed in compliance with the controller's instructions? Please explain.

Response

Yes

Justification

Data processed will be the minimum of what is needed to perform services that are required. Data access will follow the principle of least privilege so that a user can only access what they need to perform their primary job function. .
Personal Data processed will be:
- Adequate – sufficient to properly fulfill stated purpose
- Relevant – has a rational link to that purpose; and
- Limited to what is necessary – only hold the data needed for that purpose.

8.15 Are measures in place to ensure that personal data are protected against loss and destruction? Please explain.

Response

Yes

Justification

IT/IS policies/procedures are followed by all personnel.
Physical data storage is in locked area, with entry for authorized personnel only.
Data is protected during transit using HTTPS encryption

8.16 Are measures in place to ensure that personal data collected for different purposes can be processed separately? Please explain.

Response

Yes

[redacted]

onetrust

[redacted]

Assessment notes