[redacted]

[redacted]

General Data Protection Impact Assessment

Clinical studies sponsored by Janssen Pharmaceutical Companies

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
		[redacted]
[redacted]	[redacted]	[redacted]

Table of Contents

[redacted]

[redacted]

1 Purpose

The purpose of this document is to serve as a general Privacy and Data Protection Impact Assessment ("DPIA") for clinical studies sponsored by Janssen Pharmaceutical Companies in J&J, considering the standard Policies and Procedures that are applied to ensure appropriate regulations are followed for the organization, including local regulations.

For a specific clinical study or a group of similar studies a "Study Specific DPIA" will be performed in addition to this general DPIA. The purpose of the study specific DPIA is to confirm that appropriate Policies and Procedures have been applied for systems, and suppliers that will be in scope of the processing of Personal Information associated with the clinical study, and in case risks are identified, ensure that those are managed appropriately.

2 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3 [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4 [redacted]

[redacted]

[redacted]

[27] TV-SOP-12920, Study Plans and Systems During the Study Set-Up and Conduct

5 Data Protection Impact Assessment

5.1 Context

Which is the processing under consideration?

Processing of Personal Information related to clinical study participants in a clinical study sponsored by Janssen Research & Development or a local Janssen affiliate.

The processing in scope is any processing where the Sponsor[1] would be deemed a Data Controller.

Further contextual details need to be documented in the Study Specific DPIA [redacted] section 3.2.

[1] [redacted]

What are the responsibilities linked to the processing?

The global Sponsor (Legal entity owning the study protocol) is the Data Controller.

Parties that are working on behalf of the Sponsor are Data Processors. Data Processors include but may not be limited to suppliers such as hosting providers of systems used, laboratory service providers, data management providers, imaging providers and contract research organizations.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Are there standards applicable to the processing?

Each clinical study must be executed in accordance with Good Clinical Practice and applicable laws and regulations.

[redacted]

The J&J Information Asset Protection Policies (IAPPs) will apply to Personal Information that is processed. [redacted]

[redacted]

Any information will be retained as defined in the J&J Enterprise Retention Schedule.

Any supplier that is processing J&J owned information is appropriately assessed as per the Business Partner Risk Assessment process.

Any contract with suppliers that is processing Personal Information on behalf of J&J include an appropriate Privacy Exhibit, and measures for cross border transfer such as the Standard Contractual Clauses approved by the European Commission, where required.

[redacted]

[redacted]

[redacted]

What are the data processed?

Personal Information is collected as required under the study protocol.
Key-coded data, which do not contain any direct identifiers are provided to the Sponsor or parties that working on behalf of the Sponsor.

Generally Personal Information concerning health is processed. In case required considering the research objectives genetic data may be collected. Other special categories of data such as racial or ethnic origin, as well as data concerning a person's sex life or sexual orientation may be collected as well in case required for the scientific evaluation.

In certain scenarios direct identifiers of study participants may be processed by third party service providers. This would typically relate to the delivery of services to the study participants which may be required due to the specific nature of the study. Examples below:

- Name and contact information may be processed by third party services providers in case study participants may be offered (or are required) to use home nursing services, or when it is necessary to deliver medication to the study participant.
- Email address and/or phone number may be processed by third party service providers in case study participants may be offed (or are required) to use telemedicine solutions or other tools to allow study participants to utilize such technology.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

How does the life cycle of data and processes work?

The processing activities are summarized as follows:

(i) Clinical Sites, through their Principal Investigator and any investigational staff, will use Personal Information (including medical records) for study participant recruitment, eligibility, and to conduct the clinical study.

The Principal Investigator will review personal information to determine and assess suitability for study participation prior to obtaining a signed informed consent form from each clinical study participant participating in the study. Once informed consent is obtained, the Principal Investigator will obtain Personal Information of study participants and review study participants medical records to complete all necessary documents and reports required by the study protocol, including all case report forms that collect the minimum amount of data needed concerning each study participant participating in the clinical study.

The case report forms contain only pseudonymized data of study participants in the form of keycoded data ("Key-Coded Data"). Key-Coded Data is a type of pseudonymized data where Personal Information that identifies a particular clinical study participant has been replaced with a subject identification code that is not derived from information related to the individual, such that it is possible only to trace the data back to the particular data subject by referencing the key.

Case report forms are designed to collect only the minimum necessary data and only the clinical study participants identification code number and various test results or other medical information related to the clinical study. Case report forms do not contain direct personal identifiers such as name or address. The Sponsor will have enough information to differentiate data subjects but will not know (and does not need to know) the identity of the clinical study participants participating in the clinical study.

For scenarios where direct identifiers of study participants are collected, the processing of such information will be made separately from any case report forms and only to deliver specific services as may be required due to the nature of the research. E.g., in case there is a need provide a possibility for patients to do remote visits (telemedicine) or to deliver medication directly to the home a study participant the contact information such as name, email, phone number and address of such a study participant would be separately processed only as required to deliver such services. [redacted]

(ii) Monitoring and auditing of a clinical study by the Sponsor and/or parties working on behalf of the Sponsor. For the purpose of ensuring credibility of the collected clinical study data (an ICH-GCP requirement) and in accordance with the monitoring plan and applicable procedures, representatives of the Sponsor will review clinical data at each Clinical Site that contains non-pseudonymized Personal Information for purposes of study monitoring, confirming accuracy and completeness of case report forms. Such processing is limited to on-site access only, unless remote monitoring is used, and have been accepted by the relevant ethics committee. Monitors will not copy or retain any Personal Information of study participants reviewed while at a Clinical Site. As a part of the standard monitoring

[redacted]

[redacted]

[redacted]

practice, it is confirmed that study participants have signed the consent necessary considering their participation in the clinical study.

[redacted]

[redacted]

[redacted]

Clinical study data, including non-pseudonymized Personal Information may also be reviewed at each Clinical Site by regulatory authorities as permitted under ICH GCP.

(iii) Pharmacovigilance reporting. Adverse events described in the case report forms may be reported from the Principal Investigator to: The Sponsor or its third-party service providers; the Ethics Committee that is responsible for the protection of the rights and welfare of individuals participating in the clinical study; and the applicable government health authority.

(iv) Study data analysis. The Key-Coded Data will be disclosed to Sponsor and its third-party service providers for purposes of study analysis and aggregation with other Key-Coded Data collected for the clinical study.

(v) Reporting. A Clinical Study Report is generated to provide details about the methods and results of a clinical study. Such a report includes Key-Coded data and may be provided to applicable government health authorities. Transparency requirements may require that Sponsor is providing a Clinical Study Report, where the Key-Coded data has been anonymized as per applicable regulatory guidance.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5.2 Fundamental principles

5.2.1 Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

The processing purpose is clearly laid out as a part of the study protocol for each study. The necessary information is also made available to the clinical study participant as a part of the Informed Consent Process, as required by applicable regulatory requirements and Clinical SOPs.

The Clinical Study is, where required by applicable law, reviewed by an ethics committee to ensure that the study is meeting the ethics standards.

[redacted]

What is the legal basis making the processing lawful?

Consent is required to enroll a clinical study participant to a clinical study as required by the regulations and ethical standards that apply in clinical research. It should however be recognized that the consent required for a clinical study participant to be engaged in a clinical study may not be the legal ground for the processing of Personal Information in accordance with GDPR, as applicable.

Legal grounds as per GDPR article 6:

- GDPR article 6.1.c – Considering that GCP has been implemented in EU law via the Clinical Trial Directive, as well as the Pharmacovigilance Obligations that apply and the associated requirements on reliability and safety.
- GDPR article 6.1.f – For activities that are necessary for the performance of the scientific research under the study protocol, which may not be explicitly required due to the Clinical Trial Directive or other applicable laws.

Addressing the prohibition on the processing of special categories of Personal Information as per GDPR article 9:

- GDPR article 9.2.i – Considering the pharmacovigilance that the Market Authorization Holder of the Investigational Product is subject to.
- GDPR article 9.2.i – For performance of the research as described in the study protocol for each clinical study.

For processing activities, where there is no other legal ground for the processing of Personal Information consent would be the legal basis. Typically, this would involve the provision of voluntary services to study participants, which would not be mandatory for the participation in the clinical study.

It is recognized that there may be different local positions concerning the legal basis for processing Personal Information in clinical research and there is a dependency with local law. The position stated herein therefore is our general interpretation, which is in line with the European Data Protection Board opinion 3/2019.

[redacted]

[redacted]

[redacted]

Are the data collected adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')?
The data that is collected as a result of the study protocol is necessary to answer the scientific based questions which are fundamental for the Clinical Study and necessary for the execution of the study in accordance with regulatory requirements.

The statistical analysis plan provides information justifying the need for the data for the scientific evaluation of the results.

Information such as subject initials or the full date of birth is not provided to the Sponsor, unless required as per applicable law or regulation, or otherwise necessary for reasons of patient safety (personalized medicine).

[redacted]

Are the data accurate and kept up to date?
The Data Management Plan describes how data will be managed in order to ensure data integrity, and contains data review and cleaning procedures ensure data accuracy of clinical study data.

What is the storage duration of the data?
Sponsor will commonly store the data for the lifetime of the investigational product + 25 years [redacted]. This is retention of the data required according to regulatory requirements that apply in clinical research.

Depending on the specific country in scope and the nature of the study the retention time may be different than stated above.

[redacted]

5.2.2 Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?
Clinical study participants are informed about the processing of their Personal Information during the enrollment, as a part of the informed consent process. The informed consent form will describe how Personal Information will be managed, in accordance with local regulations and is approved by the relevant Ethics Committee, prior to being used.

[redacted]

[redacted]

[redacted]

How is the consent of data subjects obtained?
Consent is obtained in writing (or electronically) in accordance with requirements in ICH GCP. The Principal Investigator is responsible for collecting consent from the clinical study participant.

Please note that even though consent is collected from the clinical study participant for his/her participation in the study, consent is not always considered the legal basis for the processing of his/her Personal Information in accordance with GDPR.

How can data subjects exercise their rights of access and to data portability?
A clinical study participant has the right to provide a request to the Principal Investigator concerning access or portability of data as per applicable law. Access and portability may be limited due to other applicable regulatory requirements, e.g.in case of a blinded study. Portability only applies to data that is provided by the study participant, including lab results, and to the extent applicable as per local legal position.

[redacted]

How can data subjects exercise their rights to rectification and erasure?
The clinical study participant can contact the Principal Investigator to request to rectify and erase data.

Any changes to data need to be represented in an audit trail as a result of the requirements in Good Clinical Practice guidelines (e.g., ICH GCP Section 5.5.3). Considering that retention of data may be required under applicable law, requests for erasure may be denied.

[redacted]

Are the obligations of the processors clearly identified and governed by a contract?
The standard contracting model in J&J requires that third party service providers that may process Personal Information on behalf of a J&J affiliate, undergo an assessment (The Business Partner Risk Assessment), and that appropriate Privacy and Security language is included in the contract.

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

Transfers to external third-party service providers
Our standard contracting process require that third-party service providers in non-adequate countries are governed by an appropriate transfer mechanism such as the Standard EU Contractual Clauses.

Additional safeguards
In light of the European Court of Justice Ruling to invalidate the Privacy Shield the 16th of July 2020 there is a need to consider additional safeguards to limit any risks towards data subjects. The following are standard safeguards that J&J is applying:

- Contractual: The J&J standard privacy exhibit language includes additional contractual safeguards to prevent that data may be disclosed due to request from a surveillance authority or similar.
- IT Security: The J&J Information Asset Protection Policies would require that encryption technologies (in transit and in rest) is applied for any special categories of Personal Information / Type 3 Personal Information.

[redacted]

[redacted]

5.3 Planned or existing measures

5.3.1 Specific measures in clinical studies

Independent ethics committee or institutional review board review
Before carrying out a clinical study, an independent ethics committee or institutional board review is performed to give an opinion about whether the research is ethical, when required per applicable law. They scrutinize elements such as the proposed participant involvement, and are entirely independent of the Sponsor, funders and investigators. This enables them to put participants at the center of their review.

[redacted]

[redacted]

[redacted]

[redacted]

Pseudonymization / partitioning
As required under ICH GCP Personal Information will be coded (pseudonymized) before it is sent from the Clinical Site to the sponsor or parties working on behalf of the sponsor. The key that links the code to the name of the clinical study participant is kept at the Clinical Site.
Anonymization In certain situations, e.g., as required under European Medicines Agency (EMA) Policy 70, Personal Information that has been coded is made anonymous in accordance with applicable industry guidance, including guidance published by EMA.
Archiving Archiving is managed in accordance with the Standard Operating Procedure [redacted] which describe the activities and responsibilities related to the management of a Trial Master File (TMF). [redacted]
[redacted]

5.3.2 General Measures

Information Asset Protection Policies
[redacted].
Integrating privacy into projects
[redacted]

[redacted]

[redacted]

[redacted]

Supplier Management and Contracting Before a third-party service provider is approved to process J&J owned information a Business Partner Risk Assessment is performed to confirm that the third-party service provider is meeting the expectations in terms of IT-security and privacy. Contracting is performed using J&J templates, that include an appropriate privacy exhibit, and include, where necessary measures for cross border transfer such as the Standard EU Contractual Clauses.
Organization J&J has a global privacy team, and a network of local privacy managers.
Managing staff All J&J staff and contractors receive an annual training on IT security and privacy. Specific training is provided to key roles.
Managing Privacy Incidents Privacy Incidents are managed [redacted] [redacted]

[redacted]

[redacted]

[redacted]

5.4 Risks

5.4.1 Common risks scenarios and their associated controls

This section gives **examples of** common risks related to the processing of Personal Information, including coded data in Clinical Research and how such risks are addressed considering the policies and procedures that are applicable. (Study specific risks are listed in the study specific DPIA)

No	Risk Category	Risk Description / Scenario	Potential Impact to data subject (Study Participant)	Impact (Low, Medium, High, Very High)	Probability (Low, Medium, High, Very High)	Controls reducing the Impact and/or Probability as per J&J Policies, Procedures and Standards	Residual Risk
1	Unauthorized access to data	A Principal Investigator is getting access to the coded data of a clinical study participant in the wrong site. Main Cause: Human Error.	Not likely any impact considering the confidentiality obligations a Principal Investigator would be bound by.	Low	Low	Training, access control procedures. Privacy Incident Management, Confidentiality obligation of Principal Investigator and staff.	Low

No	Risk Category	Risk Description / Scenario	Potential Impact to data subject (Study Participant)	Impact (Low, Medium, High, Very High)	Probability (Low, Medium, High, Very High)	Controls reducing the Impact and/or Probability as per J&J Policies, Procedures and Standards	Residual Risk

[redacted]

[redacted]

2	Unauthorized access to data	A Principal Investigator or an investigational staff member do not appropriately redact information that is provided to the Sponsor or parties that are working on behalf of the Sponsor. Main Cause: Human Error.	Not likely any impact. In case of any incidental further disclosure to individuals that are not subject to confidentiality requirement, the worst-case scenario is that Directly Identifiable Health data is disclosed, which may create a risk of discrimination or embarrassment. The level of risk depends on the inclusion criteria for the study. If a study participant needs to have a pre-defined health condition the risk would be higher	Low	Medium	Training of Principal Investigator and investigational staff (General GCP Training + training awareness during Site Initiation), Privacy Incident Management	Low

No	**Risk Category**	**Risk Description / Scenario**	**Potential Impact to data subject (Study Participant)**	**Impact (Low, Medium, High, Very High)**	**Probability (Low, Medium, High, Very High)**	**Controls reducing the Impact and/or Probability as per J&J Policies, Procedures and Standards**	**Residual Risk**

[redacted]

[redacted]

3	Unauthorized access to data, Destruction, or loss of data.	A third-party service provider that is processing key-coded clinical study data is exposed to a Data Breach. Main Cause: Cyberattack, Theft or loss of device, employee data theft or data leak.	Not likely any impact, considering that no Direct Identifiers are included. The data that may be processed could be rich, which means that it contains specific health conditions, as well as dates and indirect location information (Information about Institution). As such there is a remote risk of re-identification, and in such a case it could in the worst-case scenario create a risk of discrimination or embarrassment.	Medium	Low	Business Partner Risk Assessment, Contractual Safeguards, Privacy Incident Management.	Low

No	**Risk Category**	**Risk Description / Scenario**	**Potential Impact to data subject (Study Participant)**	**Impact (Low, Medium, High, Very High)**	**Probability (Low, Medium, High, Very High)**	**Controls reducing the Impact and/or Probability as per J&J Policies, Procedures and Standards**	**Residual Risk**

[redacted]

[redacted]

4	Unauthorized access to data, Destruction or loss of data.	A third-party service provider that is processing patient data, containing directly identifiable data is exposed to a Data Breach. Main Cause: Cyberattack, Theft or loss of device, employee data theft or data leak.	There is a risk that a study participant may be subject to discrimination of embarrassment. The level of risk depends on the inclusion criteria for the study and the nature of the data that may have been compromised. If a study participant need to have a pre-defined health condition the risk would higher, as the disclosure of the name or phone number in combination with the information about the specific research could be sufficient to expose to study participant to risks. In this scenario there is also a general risk in case information such as an individual's email address or phone number is disclosed that such an individual is getting exposed to unwanted emails, phone calls or fishing attempts.	High	Low	Business Partner Risk Assessment, Contractual Safeguards, Privacy Incident Management.	Low

[redacted]

[redacted]

No	Risk Category	Risk Description / Scenario	Potential Impact to data subject (Study Participant)	Impact (Low, Medium, High, Very High)	Probability (Low, Medium, High, Very High)	Controls reducing the Impact and/or Probability as per J&J Policies, Procedures and Standards	Residual Risk
5	Unauthorized access to data, Unwanted change of data.	Login credentials are inappropriately managed at the Clinical Site, a third-party service provider or by the Sponsor. Main Cause: Human Error.	In case of deliberate intention to cause damage there is a risk that a study participant may be subject to discrimination of embarrassment. There is also a risk that data integrity may be compromised. Generally, no risk to the safety of the patient, unless in very rare situations. E.g., for research involving personalized medicine, the delivery of such medicine may be delayed.	Medium	Low	Training of Principal Investigator and any investigational staff (Site Initiation), Business Partner Risk Assessment, The J&J IAPPs, Contractual Safeguards, Training of Staff, Privacy Incident Management	Low

No	Risk Category	Risk Description / Scenario	Potential Impact to data subject (Study Participant)	Impact (Low, Medium, High, Very High)	Probability (Low, Medium, High, Very High)	Controls reducing the Impact and/or Probability as per J&J Policies, Procedures and Standards	Residual Risk

[redacted]

[redacted]

6	Unauthorized access to data	Key-coded data is distributed to the incorrect party. E.g., a third-party service provider distribute data to the wrong Sponsor. Main Cause: Human Error.	Not likely any impact, considering that no Direct Identifiers are included. The data that may be processed could be rich, which means that it contains specific health conditions, as well as dates and indirect location information (Information about Institution). As such there is a remote risk of re-identification, and in such a case it could in the worst-case scenario create a risk of discrimination or embarrassment.	Medium	Low	Business Partner Risk Assessment, Contractual Safeguards, Training of staff, Privacy Incident Management.	Low
7	Unauthorized access to data, Destruction or loss of data.	A system key-coded data has security vulnerabilities that may cause a Data Breach. Main Cause: Cyberattack.	The data that may be processed could be rich, which means that it contains specific health conditions, as well as dates and indirect location information (Information about Institution). As such there is a remote risk of re-identification, and in such a case it could in the worst-case scenario create a risk of discrimination or embarrassment.	Medium	Low	SDLC, EBIS SaaS Service Validation Process, The J&J IAPP, Privacy Incident Management, Business Partner Risk Assessment, Contractual Safeguards.	Low

[redacted]

[redacted]

No	Risk Category	Risk Description / Scenario	Potential Impact to data subject (Study Participant)	Impact (Low, Medium, High, Very High)	Probability (Low, Medium, High, Very High)	Controls reducing the Impact and/or Probability as per J&J Policies, Procedures and Standards	Residual Risk

[redacted]

[redacted]

8	Unauthorized access to data, Destruction or loss of data.	A system containing patient data, with directly identifiable data is exposed to a Data Breach. Main Cause: Cyberattack.	There is a risk that a study participant may be subject to discrimination of embarrassment. The level of risk depends on the inclusion criteria for the study and the nature of the data that may have been compromised. If a study participant need to have a pre-defined health condition the risk would higher, as the disclosure of the name or phone number in combination with the information about the specific research could be sufficient to expose to study participant to risks. In this scenario there is also a general risk in case information such as an individual's email address or phone number is disclosed that such an individual is getting exposed to unwanted emails, phone calls or fishing attempts.	High	Low	SDLC, EBIS SaaS Service Validation Process, The J&J IAPP, Privacy Incident Management, Business Partner Risk Assessment, Contractual Safeguards.	Low

[redacted]

[redacted]

No	Risk Category	Risk Description / Scenario	Potential Impact to data subject (Study Participant)	Impact (Low, Medium, High, Very High)	Probability (Low, Medium, High, Very High)	Controls reducing the Impact and/or Probability as per J&J Policies, Procedures and Standards	Residual Risk
9	Unauthorized access to data	Personal Information concerning a Study participant is disclosed to a Surveillance Authority as per Surveillance Laws (e.g., US Section 702 FISA, US Executive Order 12333, US National Security Letters). Main Cause: National Surveillance Laws and Practices.	Study participant may be subject to actions by a National Surveillance Authority, which could lead to discrimination or limitations concerning the freedom (e.g., the ability to travel to US) of the study participant.	Medium (Considering the nature of data processed)	Low	Appropriate safeguards as per GDPR Chapter V. Additional contractual safeguards as well as the application of encryption technologies.	Low
10	Unwanted change of data, Destruction or loss of data.	Data, including Personal Information in the manufacturing chain that concerns personalized medicine (e.g., CAR-T) is compromised. Main Cause: Cyberattack, Theft or loss of device,	Study participant (Patient) receives the wrong treatment, or the treatment to the study participant is delayed.	High or Very High (in case a patient gets the wrong treatment)	Low	Manufacturing process governed by robust quality standards (GMP), SDLC, EBIS SaaS Service Validation Process, The J&J IAPP, Privacy Incident Management, Business Partner Risk Assessment, Contractual Safeguards.	Low

[redacted]

[redacted]

		employee data theft or data leak.					

5.4.2 Assessment of the Risks

Risks	Accepted?	Corrective Controls
Unauthorized access to data	If the J&J Policies, Procedures and Standards are consistently applied the residual risk is low and considered acceptable. [redacted]	See table in section 5.4.1.
Unwanted change of data.	If the J&J Policies, Procedures and Standards are consistently applied the residual risk is low and considered acceptable. [redacted]	See table in section 5.4.1.

[redacted]

[redacted]

Destruction or loss of data	If the J&J Policies, Procedures and Standards are consistently applied the residual risk is low and considered acceptable. [redacted]	See table in section 5.4.1.

[redacted]

[redacted]

6 Annex 1 – DPIA Structure for Clinical Studies sponsored by Janssen Research & Development

The Privacy and Data Protection Impact Assessment model applied for Clinical Studies is consisting of different modules. This would allow assessment for each Clinical Study to be focused on 1) deviations regarding how the J&J Policies, Procedures and Standards have been applied and 2) specific risk scenarios that may occur due to the nature of the Study, or any specific service or technology that may be used.

This document (The General DPIA) is an umbrella DPIA covering a similar set of processing operations (i.e., Clinical Studies sponsored by Janssen Research & Development), which is describing how policies, procedures and standards that are applicable for Janssen Research & Development are addressing data protection and privacy related risks.

For each study an assessment is performed ("The Study Data Protection Impact Assessment") to verify that policies, procedures, and standards in place for the specific study are implemented appropriately. The focus of this activity is to ensure:

- Data collected is limited to what is necessary for the execution of the research as specified in the study protocol;
- Systems used have been implemented appropriately as per J&J standards;
- Third-party suppliers in scope for the specific study have been assessed (according to J&J´s Business Partner Risk Assessment process), and appropriate contracts are in place, including coverage for cross border transfer as needed;
- Any relevant risks are identified, and actions taken to mitigate such risks if necessary.

[redacted]

[redacted]

[redacted]

30

7 Annex 2 – Record of Processing Activities

The purpose of this annex is to describe how the Study Specific DPIA, alongside with other information is addressing the requirements in GDPR article 30.

[redacted]

[redacted]

[redacted]

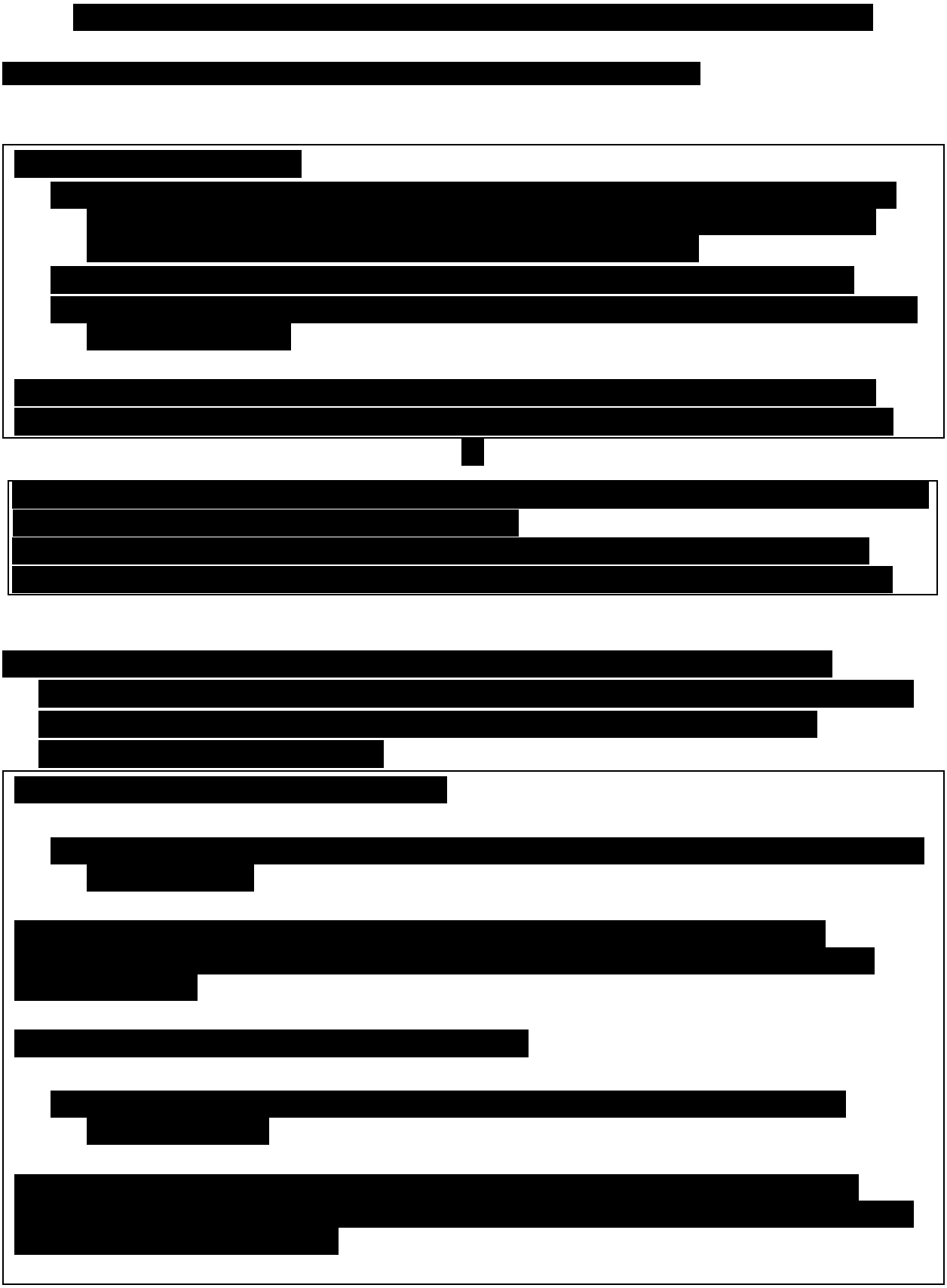
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]



[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]