

●

SANOFI Binding Corporate Rules (BCR-C)

For the transfer of Personal Data

●

Contents

PART I. BACKGROUND AND SCOPE	3
1. Purposes	4
2. Scope	4
PART II. SANOFI'S BCR COMMITMENTS	5
Section 1. Data Processing Principles	5
1. Purpose limitation	5
2. Lawfulness of the Processing Activity	5
3. Fairness and transparency	7
4. Data minimization and accuracy	7
5. Security, integrity and confidentiality	8
6. Limited retention of Personal Data	9
7. Accountability	9
8. Compliance with Personal Data Breach reporting requirements	10
9. Information and rights of Data Subjects	11
10. Ensuring adequate protection for Personal Data transfers	13
11. Action where national legislation prevents compliance with these SANOFI BCR	14
12. Compliance with these SANOFI BCR	18
13. Return or deletion of Personal Data	18
Section 2. Guarantees of bindingness, implementation & enforcement	19
14. Binding nature of these SANOFI BCR	19
15. Cooperation with Data Protection Authorities	19
16. Data Subject complaints	19
17. SANOFI BCR Update Procedure	20
18. Accessibility of these SANOFI BCR	20
19. Conflict of Law	20
20. Government requests for disclosure of Personal Data	20
Section 3. Third Party Beneficiary Rights	21
21. Third Party rights	21
22. Right to judicial, remedies & compensation	22
PART III. APPENDICES	24
Appendix 1. Definitions	24
Appendix 2. Material scope	29
Appendix 3. GDPR Provisions	36

DOCUMENT HISTORY

<i>Version</i>	<i>Application Date</i>	<i>Description</i>
1.0	2009	Initial version
2.0	2026	General update in accordance with the Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of the EDPB

Sanofi has Binding Corporate Rules (BCR) in place since 2009 to protect Personal Data across its operations worldwide. These rules are regularly updated to meet the highest data protection standards. The SANOFI BCR were first approved by the CNIL, Lead Data Protection Authority, and every update since has followed the review process required by the European General Data Protection Regulation. The most recent version was approved by the CNIL, with the European Data Protection Board (EDPB).

PART I. BACKGROUND AND SCOPE

The SANOFI Group (herein after "**SANOFI**") fully understands and values the importance of privacy and the protection of Personal Data in the digital era and is committed to ensure an adequate level of data protection for all persons with whom SANOFI has dealings.

This commitment is expressed in its Code of Ethics published on SANOFI's website¹, and its SANOFI Privacy Rules.

SANOFI obtained an approval from the Competent Data Protection Authority in 2009, SANOFI has updated its Binding Corporate Rules following the enforcement of the European General Data Protection Regulation (GDPR) to provide adequate protections for Personal Data shared among SANOFI Group.

These Binding Corporate Rules, along with their Appendices (hereinafter the "**SANOFI BCR**"), formalize SANOFI's commitment to ensure an adequate level of protection of Personal Data in accordance with the GDPR across its entire organization for the data Processing Activities described in [2. Scope](#) of these SANOFI BCR.

These SANOFI BCR describe how SANOFI will comply with Applicable Privacy Laws in respect of the processing it performs as a Data Controller.

The terms used throughout this document have specific meanings. A complete list of definitions is provided in [Appendix 1](#). Where a term is not defined there, it follows the definition set out in the GDPR.

This public version of these SANOFI BCR is available at www.sanofi.com and is maintained up-to-date. It includes in full Data Processing Principles ([Section 1](#). and Third Party Beneficiary Rights ([Section 3](#). together with selected provisions from Guarantees of bindingness, implementation & enforcement ([Section 2](#). relevant to Data Subjects, presented in a clear and accessible manner for the benefit of Data Subjects.

Contact

- Webforms available on this webpage <https://www.sanofi.com/en/data-protection-contact> , or,
- Postal mail at: EBI - Data Privacy Office, 46 Avenue de la Grande Armée 75017 Paris, France.

¹ <https://www.codeofconduct.sanofi>

1. Purposes

The purpose of these SANOFI BCR is to define the principles according to which all SANOFI BCR Members undertake to comply with when processing Personal Data governed by the GDPR and to ensure an adequate level of protection when Personal Data is transferred within the SANOFI Group from Data Importers to Data Exporters.

The implementation of these SANOFI BCR shall also serve as one of the tools to increase culture and awareness about the SANOFI Privacy Rules within SANOFI Group.

2. Scope

These SANOFI BCR cover all Processing Activities falling within the material scope and which are conducted by a SANOFI BCR Member operating as Data Controller or as Data Processor for another SANOFI BCR Member in any of the following cases:

- The SANOFI BCR Member which processes Personal Data is established in the European Union and/or in the EEA;
- The SANOFI BCR Member which processes Personal Data is established in a Third Country and has received the Personal Data from a SANOFI BCR Member established in the European Union and/or in the EEA;
- By convention between SANOFI BCR Member, any transfer of Personal Data between SANOFI BCR Members regardless of whether either entity is established within or outside the EEA;
- The Onward Transfers of Personal Data from Data Importers to Data Importers.

These SANOFI BCR apply to all SANOFI Affiliates adhering to them by the execution of the BCR Acceptation Agreement and acting as Data Exporters or Data Importers regardless of their localization and jurisdiction when processing any Personal Data as Data Controller.

These SANOFI BCR apply to any Processing of Personal Data implemented by SANOFI BCR Members in the context of:

- Managing People and Culture,
- Clinical trials and studies, Real-World Evidence studies,
- Health vigilance systems.

Where it is subject to Personal Data transfers:

- By a SANOFI BCR Member that is individually subject to EU Law;
- By a SANOFI BCR Member located in a Third Country.

A general description of the categories of Personal Data transfers governed by these SANOFI BCR is included in [Appendix 2](#). Such description covers the categories of Personal Data transfers, their purposes, the nature and the categories of Personal Data, the categories of Data Subjects, and the identification of the countries of the Data Importers.

SANOFI applies these SANOFI BCR in all cases where a SANOFI BCR Member processes Personal Data both manually and by automatic means.

These SANOFI BCR will apply to all Data Subjects – regardless of their location – whose Personal Data are transferred in the context of the Processing Activities falling within the above-defined material scope by a SANOFI BCR Member.

These SANOFI BCR do not govern the Processing Activities and Personal Data transfers which are not included in the defined material scope. Such Personal data transfers are protected using various relevant lawful mechanisms such as EU standard contractual clauses and Applicable Privacy Laws requirements.

PART II. SANOFI'S BCR COMMITMENTS

These commitments apply when SANOFI Affiliates that have adhered to these Binding Corporate Rules determine how and why Personal Data is processed (acting as a "**Data Controller**").

They establish the fundamental data privacy principles that all adhering Sanofi entities worldwide must follow when collecting, using, and transferring Personal Data within the scope of these Binding Corporate Rules. These principles are binding for all adhering Sanofi entities across the entire SANOFI Group.

They also outline the operational measures Sanofi has put in place to ensure these rules are properly applied and enforced within all adhering entities, including the commitments SANOFI has made to Data Protection Authorities.

Finally, they detail the specific rights individuals have under these Binding Corporate Rules and how to exercise them. These rights apply regardless of where personal data is processed within the adhering SANOFI entities.

Section 1. Data Processing Principles

Data Importers and Data Exporters shall ensure that all Processing Activities carried out within the SANOFI Group are designed, implemented and monitored in accordance with SANOFI data protection principles as set forth in SANOFI Privacy Rules. In any event, Personal Data shall be Processed in accordance with Applicable Privacy Laws.

In particular, all Data Exporters and Data Importers must comply with the following principles:

1. Purpose limitation

- 1.1 SANOFI BCR Members must at all times ensure that the Processing of Personal Data is carried out for a specified, explicit and legitimate purpose and limited to what is necessary.
- 1.2 SANOFI BCR Members will only process Personal Data for said specified, explicit and legitimate purposes and not further process that information in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes, provided that appropriate technical and organizational safeguards are implemented to protect Data Subject's rights and freedoms.

2. Lawfulness of the Processing Activity

- 2.1 SANOFI BCR Members must at all times ensure that the Processing of Personal Data has a lawful basis in compliance with any Applicable Privacy Laws, including any laws governing the protection of Personal Data in the country where Personal Data are originally collected.
- 2.2 Lawful Processing of Personal Data means that SANOFI BCR Members will process Personal Data falling within the scope of these BCR only if at least one of the following conditions established by EU Law, is met:
 - The Data Subject has consented to the Processing of its Personal Data for one or more specific purposes.
 - The Processing of Personal Data is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.

The Processing of Personal Data is necessary for compliance with a legal obligation the Data Controller is subject to under Applicable Privacy Laws.
 - The Processing of Personal Data is necessary in order to protect vital interests, such as life, health or safety, of the Data Subject or of another individual.
 - The Processing of Personal Data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

- The Processing of Personal Data is necessary for the purposes of legitimate interests pursued by the Data Controller or by a Third Party, except where such interests are overridden by the interests or fundamentals rights and freedoms of the Data Subject.
- 2.3 To this end, SANOFI BCR Members shall only process Personal Data relying on one of the legal bases as detailed in [Appendix 2](#).
- 2.4 Where a Processing Activity involves the processing of Sensitive Personal Data, SANOFI BCR Members shall:
- Rely on an adequate basis as listed in [2.5](#),
 - Conduct a Privacy Risk Assessment if necessary and include appropriate measures to preserve the rights of the individuals, without prejudice to compliance with the other principles set out in these SANOFI BCR.
- 2.5 Processing of Sensitive Personal Data are subject to additional requirements due to higher risk for an individual if misused or processed incorrectly. Where a SANOFI BCR Member Processes Sensitive Personal Data, it will only do so, if:
- The Data Subject has given explicit consent to the Processing of those Personal Data for one or more specified purposes, except where the EU Law provides that the prohibition of Processing Sensitive Personal Data may not be lifted by the Data Subject;
 - The Processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the Data Controller in the field of employment and social security and social protection law in so far as it is authorized by the EU Law or by a collective agreement pursuant to the EU Law providing for appropriate safeguards for the fundamentals rights and the interests of the Data Subject;
 - The Processing is necessary to protect vital interests of the Data Subject of another natural person where the Data Subject is physically or legally incapable of giving consent;
 - The Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the Data Subject;
 - The Processing relates to Sensitive Personal Data which are manifestly made public by the Data Subject;
 - The Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
 - The Processing is necessary for reasons of substantial public interest, on the basis of the EU Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
 - The Processing of Sensitive Personal Data is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Applicable Privacy Laws or rules established by competent bodies and EEA or EU Member State or by another person also subject to an obligation of secrecy under Applicable Privacy Laws or rules established by competent bodies in an EEA or EU Member State;
 - The Processing of Sensitive Personal Data is necessary for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medical products or medical devices, on the basis of Applicable Privacy Laws which provide for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy;

- The Processing of Sensitive Personal Data is necessary for archiving purposes in the public interest, scientific or historical researches or statistical purposes in accordance with article 89(1) of the GDPR² based on the EU Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interest of the Data Subject ;
- The Processing of criminal convictions and offences is strictly limited to cases where it is explicitly authorized or required by EEA or the EU Law.

2.6 Notwithstanding anything to the contrary herein, where the laws applicable to the Data Exporter provide for a broader definition, scope, or regulatory framework concerning Sensitive Personal Data, such data shall be classified as Sensitive Data, and the relevant provisions of the Data Exporter's local laws shall supersede any less protective provisions.

3. Fairness and transparency

- 3.1 Each Processing Activity must be carried out in accordance with the transparency principle and be associated to an adequate notice of information describing its specificities in accordance with the mandatory mentions as listed in the principle "*Information and rights of Data Subjects*" (see. 9.1 and 9.4) of these SANOFI BCR. Such notice of information shall contain adequate information concerning applicable Personal Data transfers and information regarding Data Subjects Rights.
- 3.2 Where the legal basis of the Processing Activity is the individual consent of Data Subjects (e.g., processing of Sensitive Personal Data) such consent must be given freely, and must be specific, informed and unambiguous prior to the implementation.

4. Data minimization and accuracy

- 4.1 Each Processing Activity must be carried out relying on Personal Data which is accurate, relevant and strictly necessary to achieve the purpose of the Processing for which it is collected.
- 4.2 SANOFI BCR Members collect the minimum amount of Personal Data necessary to pursue each specified, explicit and legitimate business purpose described in accordance with the material scope of these SANOFI BCR (See [Appendix 2](#)).
- 4.3 Where Personal Data is inaccurate or incomplete, SANOFI BCR Members shall take reasonable steps to rectify, erase or supplement such Personal Data.
- 4.4 SANOFI BCR Members will assess whether Sensitive Personal Data is required for the intended purpose of processing before collecting it.
- 4.5 As a general rule, SANOFI BCR Members:
- Do not process any Personal Data relating to criminal convictions and offences, unless it is explicitly authorized or required by EEA or EU Law;
 - Consider and assess the possibility to use anonymized or pseudonymized data, provided that the cost and effort involved is commensurate with the desired purpose.

² See [GDPR Provisions](#)

5. Security, integrity and confidentiality

5.1 The SANOFI BCR Member shall be responsible for, and be able to demonstrate compliance with, adequate technical and organizational measures that must be implemented to ensure the security and confidentiality of the Personal Data processed for each Processing Activity conducted by SANOFI BCR Members, taking into consideration the risks for the rights and freedoms of natural persons, associated with the processing Activity for the Data Subject and, in particular, with regards to the processing of Sensitive Personal Data.

To this end, SANOFI BCR Members will :

- Comply with the policies adopted for the security, safety and confidentiality of their systems, premises and data, as revised and updated from time to time,
- Implement any other security procedures relevant to any of their business areas or functions to protect the data against unlawful or unauthorized access or use, notably to prevent the occurrence of a Personal Data Breach,
- Maintain documented evidence of such compliance and regularly review the effectiveness of these measures,
- Ensure that any Employee who has access to Personal Data will do so on instructions from a SANOFI BCR Member Where a SANOFI BCR Member acting as Data Controller will only appoint a Third Party acting as Data Processor (e.g., service provider) providing sufficient guarantees to implement appropriate technical and organizational measures including security measures governing the outsourced Processing of Personal Data to be carried out and must ensure compliance with the Applicable Privacy Laws.

The SANOFI BCR Member shall document the assessment of such guarantees and maintain records of all due diligence performed.

5.2 The Processing of Personal Data by a Data Processor must be governed by written contractual terms (i.e., by an Adequate Privacy Agreement). The contractual terms will instruct the Data Processor and stipulate, in particular, that it shall:

- Maintain and make available to the SANOFI BCR Member comprehensive documentation demonstrating its compliance with these obligations;
- Act only in accordance with the SANOFI BCR Member's instructions when Processing Personal Data, including with regard to Personal Data transfers and promptly inform the SANOFI BCR Member if it considers that an instruction infringes EU Law or Applicable Privacy Laws provisions;
- Ensure that any individuals who have access to the Personal Data are subject to a duty of confidentiality;
- Only engage a sub-processor if the SANOFI BCR Member has given its prior specific or general written authorization, and on condition the sub-processor agreement protects the Personal Data to the same standard required of the service provider. In the case of general written authorization, the Data Processor shall inform the SANOFI BCR Member acting as Data Controller of any intended changes concerning the addition or replacement of sub-processors, thereby giving the said SANOFI BCR Member the opportunity to object to such changes;
- Assist the SANOFI BCR Member in ensuring compliance with its obligations as a Data Controller under Applicable Privacy Laws, in particular with respect to reporting data security incidents and responding to requests from individuals to exercise their data protection rights;
- Taking into account the nature of the Processing of Personal Data, assist the SANOFI BCR Member by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the SANOFI BCR Member's obligations to complete Data Subject requests to exercise the Data Subject's Rights;

- Return or delete the Personal Data and any existing copies at the choice of the Data Controller once it has completed its services; and

Make available to the SANOFI BCR Member all information it may need in order to ensure its compliance with these obligations and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes the EU Law or other Applicable Privacy Laws;

- Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account the state of art, the costs of implementation and the nature, scope, context and purposes of the Processing of Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

6. Limited retention of Personal Data

- 6.1 Each Processing Activity must be carried out for a defined or definable term so that Personal Data is not processed and retained for longer than strictly necessary to achieve the defined purpose of the Processing.
- 6.2 Each SANOFI BCR Member will comply with SANOFI's Retention Schedule and Policy Center and guidelines as revised and will provide adequate information to Data Subjects on the defined or definable term of retention of their Personal Data.

7. Accountability

- 7.1 SANOFI shall ensure that the Processing Activity is registered or covered by an existing register of processing activity entry in the Privacy Management System and is maintained up-to-date in accordance with related SANOFI Privacy Rules.
- 7.2 Each SANOFI BCR Member acting as Data Controller, under the supervision of the Privacy Officer shall maintain a record of the Processing Activities under its responsibility. The SANOFI BCR Member will make them available to the Data Protection Authorities upon request. The Register of Processing Activities should be maintained in writing (including electronic form). These records must contain at least the following information:
 - The identity of the SANOFI BCR Member(s) which is (are) the Data Controller(s),
 - The purpose(s) of the Processing Activity,
 - The categories of Data Subjects,
 - The categories of Personal Data,
 - The categories of Recipients to whom the data are disclosed,
 - Personal Data transfers and the Third Country(ies) where Personal Data is transferred and the relevant legal mechanism used for that purpose, and,
 - Where possible the envisaged period of retention, and a general description of the technical and organizational measures applied to the Processing Activities.
- 7.3 Each SANOFI BCR Member acting as Data Processor regardless of its geographical location, under the supervision of the Privacy Officer shall maintain a record of the Processing Activities it implements. The SANOFI BCR Member will make them available to the Data Protection Authorities upon request.

The Register of Processing Activities should be maintained in writing (including electronic form). These records must contain at least the following information:

- The identity of the SANOFI BCR Member(s) which is (are) the Data Controller(s),
- The categories of the Processing Activities,
- Personal Data transfers and the Third Country(ies) where Personal Data is transferred and the relevant legal mechanism used for that purpose, and,
- Where possible the envisaged period of retention, and a general description of the technical and organizational measures applied to the Processing Activities.

- 7.4 SANOFI BCR Members shall implement *Privacy-by-Design* and *Privacy by Default* principles for any new project (e.g., systems and applications). To that end, each Processing Activity should by default implement the most data protection-friendly settings with a view to implement the objective of data protection-by-default. SANOFI BCR Members shall at the time of the determination of the means of the processing and at the time of the processing itself, implement appropriate technical and organizational measures which are designed to implement these SANOFI BCR in an effective manner and to integrate the necessary safeguards into the processing. In addition, SANOFI BCR Members shall implement appropriate technical and organizational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed.
- 7.5 SANOFI BCR Members will carry out a Privacy Risk Assessment using the appropriate assessment module based on the nature of the Processing Activity (general or specific to the activity), and their respective qualification under the Register of Processing Activities (e.g., Data Controller, Data Processor or Joint Controller). This assessment focuses on the impact of the envisaged processing operations on the protection of Personal Data, taking into account the nature, scope, context and purposes of the Processing Activity.
- This assessment aims to address any risk and identify additional security measures and/or mechanisms to *ensure* an appropriate level of protection of Data Subjects' rights and freedoms, including the implementation of supplementary measures as specified in [Principle 11](#) where applicable. It focuses on the impact of the envisaged processing operations on the protection of Personal Data, taking into account the nature, scope, context and purposes of the processing.
- 7.6 SANOFI BCR Members shall seek the advice of the Data Protection Officer and where a Privacy Risk Assessment indicates that the Processing Activity would result in a high risk in the absence of measures taken to mitigate the risk, SANOFI will consult the Competent Data Protection Authority prior to implement such processing.

8. Compliance with Personal Data Breach reporting requirements

- 8.1 In the case that a Personal Data Breach is detected, such incident shall be managed by the SANOFI Personal Data Breach Privacy Process.
- 8.2 The SANOFI BCR Member(s) and Privacy Officer(s) as well the Business Operational Team will review the nature and seriousness of the incident and determine whether the likely consequences and/or risks on Data Subjects' rights and freedom, the measures taken or proposed to mitigate the possible effects and it is necessary under the EU Law to notify the Competent and/or Lead Data Protection Authority(ies) under seventy-two (72) hours and, where applicable, communicate without undue delay to the Data Subjects.
- 8.3 The Privacy Officer(s) and Business Operational Team shall be responsible:
- Where applicable, for ensuring the said notification to the Competent Data Protection Authority without undue delay and no later than seventy-two (72) hours after having become aware of the incident, unless it is unlikely to result in a risk to the rights and freedoms of Data Subjects;
 - Notify without undue delay any Personal Data Breach to relevant SANOFI Liabe BCR Member(s) and the SANOFI BCR Member acting as Data Controller when the Personal Data Breach is identified by a SANOFI BCR Member acting as Data Processor;
 - Where applicable, for ensuring the notification to the Data Subjects affected by the Personal Data Breach if such incident is likely to result in a high risk to the rights and freedoms in accordance with Applicable Privacy Laws;
 - To ensure that all information pertaining to the breach, its effects, remediation measures and notifications is documented and made available to the Competent and/or concerned Data Protection Authority(ies) on request.

9. Information and rights of Data Subjects

- 9.1 When a SANOFI BCR Member collects Personal Data directly from a Data Subject, it shall promptly inform the individual of the following information at the time of the data collection: the Data Controller's identity and data protection officer's contact details, the purposes and legal basis for Processing, the Recipients or categories of Recipients, any intended transfers, the retention period, and the Data Subject's rights as listed in 9.4.

This information requirement does not apply when the Data Subject already processes all of the above information.

- 9.2 When a SANOFI BCR Member obtains Personal Data through means other than direct collection from the Data Subject, it shall inform the individual of the following information: the Data Controller's identity and Data protection officer's contact details, Processing purposes and legal basis, categories and the sources of Personal Data concerned, Recipients or categories of Recipients, any intended data transfers, retention period, and the Data Subject's rights as listed in section 9.4. This information shall be provided within a reasonable period after obtaining the Personal Data, at the latest within one month, or at the time of the first communication with the Data Subject or first disclosure to another Recipient.

- 9.3 SANOFI BCR Member acting as Data Controller will not provide such information to the Data Subject where there is a legitimate basis for not doing so (including national security or defense requirements, crime prevention or detection, legal proceedings, professional secrecy obligations, legal permissions, or when providing information is impossible or would require disproportionate effort) and where the individual already has received or has access to such information.

SANOFI BCR Member acting as Data Controller shall be exempt from providing such information to the Data Subject in the following cases:

- Where a legitimate basis exists, including national security or defense requirements, crime prevention or detection, legal proceedings, professional secrecy obligations, or other legal permissions;
- Where providing the information proves impossible or would require disproportionate effort; or
- Where the Data Subject already has received or has access to such information.

- 9.4 Upon request, a Data Subject shall have the right to exercise the rights granted by Applicable Privacy Laws against any SANOFI BCR Member. Where and to the extent that Applicable Law provides for it or where EU Law applies as per the provisions of these BCRs, every Data Subject has the right to:

- Obtain confirmation whether a Data Controller processes Personal Data about them and, if so, to be provided with details of that Personal Data and access to it (*Right of Access*).
- Require from a Data Controller to:
 - o Rectify without undue delay any inaccurate Personal Data and complete incomplete data, taking into account the purpose of the Processing Activity (*Right of Rectification*);
 - o Restrict the Processing Activity (*Right of Restriction*) where:
 - The accuracy of Personal Data is contested by the Data Subject, for a period enabling the Data Controller to verify the accuracy of the Personal Data;
 - The processing is unlawful but the Data Subject opposes erasure and requests restriction instead;
 - The Data Controller no longer needs the Personal Data but they are required by the Data Subject for the establishment, exercise or defense of legal claims; or
 - The Data Subject has objected to processing pending verification of whether the Data Controller's legitimate grounds override those of the Data Subject.

When Processing Activity is restricted, such Personal Data shall, with the exception of storage, only be processed:

- With the Data Subject's consent; or
 - For the establishment, exercise or defense of legal claims; or
 - For the protections of the rights of another natural or legal person; or
 - For reasons of important public interest.
- o Erase Personal Data (*Right of Erasure*) without undue delay where:
 - The Personal Data are no longer necessary for the original purposes which they were collected or otherwise processed;
 - The Data Subject objects and there are no overriding legitimate grounds;
 - Consent is withdrawn and no other legal basis exists;
 - The Processing Activity is unlawful;
 - Erasure is required by legal obligation to which the Data Controller is subject;
 - The Personal Data have been collected in relation to the offer of information society services to children.

The right of erasure does not apply where processing is necessary for:

- Exercising the right of freedom of expression and information,
- Compliance with a legal obligation which requires the processing,
- Reasons of public interest in the area of public health,
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, insofar as the right of erasure would render impossible or seriously impair the achievement of the objectives of that processing; or
- The establishment, exercise or defense of legal claim.

When the Right of Rectification, Restriction or Erasure are exercised, the SANOFI BCR Member shall notify all recipients to whom Personal Data have been disclosed, unless such notification proves impossible or involves disproportionate effort, and shall inform the Data Subject about those recipients upon request.

- Object, at any time on grounds relating to their particular situation, to the Processing of their Personal Data based on the performance of a task carried out in the public interest or the legitimate interests of the SANOFI BCR Member or Third Party. The SANOFI BCR Member shall no longer process the Personal Data unless it demonstrates legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of legal claims (*Right of Objection*).
- Receive the Personal Data, which has been processed by SANOFI BCR Member(s), in a structured, commonly used and machine-readable format and to transmit that information to another Data Controller, if certain grounds apply (*Right to Portability*).
- Withdraw their consent at any time where the Processing of Personal Data is based on the consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before the withdrawal.
- Not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, the right to contest the decision and to require a human review of the decision (*The right not to be subject to decisions based solely on automated processing including profiling*). This right does not apply where the decision is:
 - o Necessary for entering into or performing a contract between the Data Subject and the Data Controller;

- Authorized by EU Law, to which the SANOFI BCR Member acting as Data Controller is subject and which also lays down suitable measures safeguards for the Data Subject's rights and freedoms and legitimate interests;
- Based on the Data Subject's explicit consent.

Where automated decision-making is permitted, the Data Subject has the right to:

- Obtain human intervention from the Data Controller;
- Express their point of view and contest the decision;
- Receive meaningful information about the logic involved in the automated processing, as well as an explanation of the decision reached and the significance and envisaged consequences of such Processing Activity for the Data Subject.

Automated decisions shall not be based on Sensitive Personal Data unless one of the following conditions is met:

- The Data Subject has given explicit consent for one or more specified purposes, except where EU Law provides that the prohibition may not be lifted by the Data Subject's consent; or
- The Processing Activity is necessary for reasons of substantial public interest on the basis of EU Laws which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the Data Subject's rights and freedoms and legitimate interests.

Each SANOFI BCR Member shall implement appropriate technical and organizational measures, including safeguards, to ensure accuracy of Personal Data used in automated decision-making and to prevent discriminatory effects.

9.5 Where and to the extent that Applicable Law provides for it or where EU Law applies as per the provisions of these BCR, every Data Subject has the right to:

- Submit a Data Subject Request regarding the Processing of Personal Data within the scope of these SANOFI BCR. The request shall be managed in accordance with the SANOFI Privacy Rules by the SANOFI BCR Member.
- Lodge a complaint with the Competent Data Protection Authority regarding the Processing of Personal Data within the scope of these SANOFI BCR. The request shall be managed in accordance with the SANOFI Privacy Rules by the SANOFI BCR Member.

10. Ensuring adequate protection for Personal Data transfers

10.1 SANOFI will not transfer Personal Data toward Third Country without ensuring adequate protection in accordance with the standards set out by these SANOFI BCR

In principle, transborder Personal Data transfers to a Third Country and/or Third Party located in a Third Country are not allowed without an appropriate framework or justification as provided for under Applicable Privacy Laws, such as, for instance, signing standard contractual clauses, which will protect the Personal Data being transferred.

No SANOFI BCR Member may transfer Personal Data internationally unless and until such measures as are necessary to comply with laws governing Personal Data transfers have been satisfied in full, including with respect to Onward Transfers from a Third Country.

10.2 SANOFI will ensure the adequate protection of any Personal Data that may be onward transferred outside the EEA

SANOFI BCR Member shall ensure that any Personal Data that has been transferred under these SANOFI BCR are only onward transferred outside the EEA to Third Parties if one of the following conditions is met, in accordance with the EU Law:

- The transfer is made to a Third Country recognized by the European Commission as ensuring an adequate level of protection, or,
- The transfer is subject to safeguards essentially equivalent to those guaranteed by EU Law, taking into account the specific circumstances of the Onward Transfer.

In exceptional circumstances, where the Onward Transfer cannot rely on a adequacy appropriate safeguards under Applicable Data Privacy Laws, the transfer may only take place if one of the following primary derogations applies:

- The Data Subject has explicitly consented to the proposed transfer after being clearly informed of the possible risks;
- The transfer is necessary for the performance of a contract between the Data Subject and the Data Exporter, or for implementing pre-contractual measures;
- The transfer is necessary for the conclusion or performance of a contract concluded in the Data Subject's interest between the Data Exporter and another party;
- The transfer is necessary for important reasons of public interest recognized under EU Law
- The transfer is necessary for the establishment, exercise or defense of legal claims;
- The transfer is necessary to protect vital interests of the Data Subject or other persons, where the Data Subject is physically or legally unable to give consent;
- The transfer is made from a register which, according to EU Law, is intended to provide information to the public.

Or, if none of the above derogations applies, the transfer may exceptionally take place only if:

- The transfer is not repetitive;
- Concerns only a limited number of Data Subjects;
- Is necessary for compelling legitimate interests pursued by the Data Exporter;
- Includes appropriate safeguards; and
- the competent Data Protection Authority is informed.

In all cases, any Onward Transfer shall ensure continuous protection of Personal Data at a level essentially equivalent to that guaranteed by EU Law throughout the entire transfer chain.

11. Action where national legislation prevents compliance with these SANOFI BCR

11.1 Assessment of Third Country laws and practices

SANOFI BCR Members will monitor developments in Third Countries that may affect the assessment of the level of protection and the decisions taken accordingly regarding Personal Data transfers to such countries.

Before transferring Personal Data to a Third Country, a SANOFI BCR Member acting as the Data Exporter shall assess whether the laws and practices of such country, including any requirements to disclose Personal Data or measures authorizing access by public authorities, prevent the SANOFI BCR Member from acting as the Data Importer from fulfilling its obligations under these SANOFI BCR.

This assessment shall be based on the understanding that the laws and practices of a Third Country that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society, shall not contradict these SANOFI BCR.

Furthermore, such assessment shall be based on the understanding that laws and practices of the third country of destination respect the fundamental rights and freedoms of the Data Subject and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the following objectives:

- National security;
- Defense;
- Public security;
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- Other important objectives of general public interest, in particular, important economic or financial interests, including monetary, budgetary and taxation matters, public health and social security;
- The protection of judicial independence and judicial proceedings;
- The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- Monitoring, inspection or regulatory functions connected to the exercise of official authority in the cases referred to in the preceding objectives;
- The protection of the Data Subject or the rights and freedoms of others; and/or
- The enforcement of civil law claims.

SANOFI BCR Members will document the assessment and make it available to the relevant Liable SANOFI BCR Member and, upon request, to the Competent Data Protection Authority. In assessing the laws and practices of a Third Country which may affect the respect of the commitments contained in these SANOFI BCR, SANOFI BCR Members shall take due account, in particular, of the following elements:

- The specific circumstances of the Personal Data transfers or set of Personal Data transfers, and the envisaged Onward Transfers within the same Third Country or to another one, including the purposes of the Personal Data transfer, the SANOFI BCR Members and further Recipients who are involved, the economic sector in which the Personal Data transfer occurs, the categories and format of data transferred, the location of the Processing Activity, and the transmission channels that are used to transfer the Personal Data;
- The relevant laws and practices of the Third Country in light of the circumstances of the Personal Data transfer, including any requirements to disclose Personal Data to public authorities and those providing access to data in transit, as well as the applicable limitations and safeguards; and
- Any relevant contractual, technical or organizational safeguards that may need to be implemented to supplement these SANOFI BCR, including measures applied during the transmission and to the processing of the Personal Data in the country of destination.

If a SANOFI BCR Member acting as Data Importer has reasons to believe that it is or has become subject to laws that would prevent it from fulfilling its obligations under these SANOFI BCR, including following a change in the laws of a Third Country or a measure indicating an application of such laws in practice that is not in line with these SANOFI BCR, the said SANOFI BCR Member will promptly inform:

- The SANOFI BCR Member(s) located in EU acting as Data Exporter(s),
- The SANOFI Data Privacy Office, including relevant Privacy Officer(s),
- The relevant Liable SANOFI BCR Member(s).

11.2 Identification and implementation of supplementary measures to be adopted by the SANOFI BCR Members acting as Data Exporter and/or Data Importer in order to enable them to fulfil their obligations under these SANOFI BCR in accordance with EDPB Recommendations 1/2022

Whenever there is a need to implement safeguards or supplementary measures (e.g., technical or organizational measures to ensure security and confidentiality) in addition to those envisaged under these SANOFI BCR, the SANOFI BCR Member acting as the Data Exporter shall inform the Liable SANOFI BCR Member acting as Data Importer and competent Privacy Officers of the identified measures to be adopted to address the situation.

Each SANOFI BCR Member part of the operational team, with the support of the SANOFI Data Privacy Office and relevant Privacy Officer(s), shall assess and document the assessments appropriately, including the supplementary measures selected and implemented.

SANOFI BCR Members will document the assessment and make it available to the Liable SANOFI BCR Member and, upon request, to the Competent Data Protection Authority.

The SANOFI Data Privacy Office shall inform all SANOFI BCR Members of the results of said assessment, so that any identified supplementary measures can be applied in case the same type of Personal Data transfers are carried out, or where it is not possible to implement effective supplementary measures, the Personal Data transfers at stake may be suspended or ended. Upon verification of such information, the SANOFI BCR Member acting as the Data Importer shall commit to promptly implement defined supplementary measures or identify additional measures if needed in order to enable them to fulfil their obligations under these SANOFI BCR.

SANOFI BCR Members acting as Data Importers shall promptly notify the relevant Data Exporter if, when using these SANOFI BCR as a tool for Personal Data transfers, they have reason to believe that they are or have become subject to laws or practices that would prevent them from fulfilling their obligations under these SANOFI BCR, including following changes in the laws in the Third Country or specific measures (such as a Personal Data Disclosure Request).

Upon verification of such notification, the SANOFI BCR Member acting as the Data Exporter, along with the SANOFI Data Privacy Office and the Liable SANOFI BCR Member, shall commit to promptly identify supplementary measures (e.g., technical or organizational measures to ensure security and confidentiality) to be adopted by the SANOFI BCR Member(s) acting as the Data Exporter(s) and Data Importer(s) respectively, in order to enable them to fulfil their obligations under these SANOFI BCR. The same applies if a SANOFI BCR Member acting as Data Exporter has reasons to believe that a SANOFI BCR Member acting as its Data Importer can no longer fulfil its obligations under these SANOFI BCR.

Where the SANOFI BCR Member acting as the Data Exporter, along with the relevant Privacy Officers and the liable SANOFI BCR Member, assesses that the Data Importer cannot comply with these SANOFI BCR, despite the supplementary measures implemented, or when instructed by a Competent Data Protection Authority, it shall immediately:

- Suspend the Personal Data transfer at stake,
- Suspend all other transfer for which the same assessment and reasoning would lead to a similar result,
- Maintain such suspension until compliance is again ensured or the Personal Data transfer is ended.

If compliance with these SANOFI BCR cannot be restored within one (1) month of suspension, as Data Exporter shall end the Personal Data transfer or set of Personal Data transfers. Any Personal Data that was transferred prior to this suspension (and any copies thereof) should (at the choice of the Data Exporter) either be returned or destroyed.

SANOFI BCR Members acting as Data Exporters shall monitor on an ongoing basis, and where appropriate in collaboration with the relevant Data Importers, the developments in the Third Countries to which the Data Exporters have transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such Personal Data transfers.

In case of doubt with regards to the interpretation of Applicable Privacy Laws, the Local Privacy Officer and/or the SANOFI Data Privacy Office shall seek advice from Data Protection Authorities or external counsels in order to ensure compliance with the most stringent provisions.

11.3 Management of Personal Data Disclosure Request by a public authority

Notification obligation. Subject to applicable laws, the SANOFI BCR Member acting as a Data Importer shall promptly notify the Data Exporter, the Data Privacy Office and, where possible, the Data Subject (with the support of the Data Exporter) if it:

- Receives a legally binding request from a public authority under the laws of the country of destination, or of another Third Country, for disclosure of Personal Data transferred pursuant to these BCR (e.g., law enforcement authority or state security body).
- Becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these binding corporate rules.
- Becomes aware of any receipt by a Third Party (i.e., service providers, vendors, partners) of a legally binding request by a public authority under the laws of the country in which the Third Party is located, for disclosure of information and/or Personal Data that has been transferred by SANOFI BCR Member pursuant to appropriate safeguard implemented in the agreement or other binding document.

Content of notification. Such notification shall include all information available to the Data Importer about the Personal Data requested, the identity of the requesting authority, the legal basis for the request and the draft response.

If prohibited from notifying the Data Exporter and/or the Data Subject, the Data Importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible. The Data Importer will document such efforts and demonstrate them upon request of the Data Exporter.

To the extent that it receives any Personal Data disclosure requests from a public authority, and as relevant, the Data Importer will provide periodic reports to the Data Exporter detailing all received requests including relevant information as possible. If prohibited from sharing this information, the Data Importer will promptly notify the Data Exporter and the Chief Privacy Officer of such restriction.

The Data Importer will preserve all information about requests for as long as the Personal Data are subjected to these Sanofi BCR and shall make it available to the Competent Data Protection Authority upon request.

Legal assessment. The Data Importer will review the legality of each disclosure request. The review will specifically examine whether the request remains within the powers granted to the requesting public authority. After a careful assessment, the SANOFI BCR Member acting as Data Importer will challenge the request if it finds reasonable grounds to consider it unlawful under the local laws, international obligations or principles of international comity. Under the same conditions, it will pursue possibilities of appeal, and seek interim measures to suspend its effects until a competent judicial authority has decided on its merits. The Data Importer will not disclose the requested Personal Data until required by applicable procedural rules.

The Data Importer will document all legal assessments and challenges to requests, make this documentation available to the Data Exporter and upon request, to the Competent Data Protection Authorities.

In no event shall a SANOFI BCR Member transfer Personal Data to any public authority in a Third Country in a massive, disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society. Furthermore, when responding to a request for disclosure, the Data Importer will provide the minimum amount of information permissible, based on a reasonable interpretation of the request. This approach ensures that any disclosure remains proportionate and limited to what is strictly necessary.

For SANOFI BCR Members located in the EEA, any court judgment or tribunal ruling, as well as any decision by an administrative authority of a third country that requires a Data Controller or Data Processor to transfer or disclose Personal Data, can only be recognized or enforced if it is

based on an international agreement, such as a mutual legal assistance treaty, that is in force between the requesting third country and the EU or an EEA Member State. This is without prejudice to other grounds for transfer under Chapter V of the GDPR.

If any legal requirement a SANOFI BCR Member is subject to in a Third Country is likely to significantly undermine the guarantees provided by these SANOFI BCR, the Data Importer must promptly notify the Chief Privacy Officer and the Data Exporter. The Chief Privacy Officer shall then notify the Competent Data Protection Authority and, where possible, the Data Subjects. This includes:

- Any legally binding Personal Data Disclosure Request for disclosure of Personal Data by a public authority. In such cases, the Competent Data Protection Authority must be clearly informed about the request, including details about the data requested, the requesting authority, the legal basis for the disclosure, and the response provided (unless prohibited by law, such as a criminal law prohibition to maintain the confidentiality of a law enforcement investigation), and
- Any direct access by public authorities to Personal Data transferred under these SANOFI BCR according to the Applicable Privacy Laws of the Data Importer. Such notification must include all available information (unless prohibited by law, such as a criminal law prohibition to maintain the confidentiality of a law enforcement investigation).

12. Compliance with these SANOFI BCR

- 12.1 No Personal Data transfer shall be made to a SANOFI BCR Member acting as a Data Importer unless such entity is effectively bound by these SANOFI BCR and can deliver compliance.
- 12.2 A SANOFI BCR Member acting as Data Importer shall promptly inform the Data Exporter if it is unable to comply with these SANOFI BCR, for whatever reason, including the reasons described under [Principle 11](#).
- 12.3 Where a Data Importer is found to be in breach of these SANOFI BCR or is unable to comply with them, the SANOFI BCR Member acting as a Data Exporter shall suspend the Personal Data transfer.

13. Return or deletion of Personal Data

- 13.1. A SANOFI BCR Member acting as a Data Importer should, at the choice of the Data Exporter, immediately return or delete all Personal Data in its possession that has been transferred under these SANOFI BCR (including any copies thereof) if:
 - The Data Exporter has suspended the Personal Data transfer and compliance with these SANOFI BCR is not restored within a reasonable time, and in any event within one (1) month of the suspension decision; or
 - The Data Importer is in substantial or persistent breach of these SANOFI BCR; or
 - The Data Importer fails to comply with a binding decision of a competent court or Competent Data Protection Authority regarding its obligations under these SANOFI BCR.
- 13.2. In all cases, where a SANOFI BCR Member acting as a Data Importer ceases to be able to comply with these principles and these SANOFI BCR or ceases to be bound by them, or where otherwise requested by the SANOFI BCR Member acting as Data Exporter, the Data Importer will:
 - inform the Data Exporter without delay;
 - Upon instruction from the Data Exporter, the Data Importer may keep, cease the Processing of Personal Data, return or delete all Personal Data and any copies thereof;
 - Ensure that any Third Party to whom the Personal Data has been disclosed complies with the same obligations regarding the return or deletion of the Personal Data, including any copies thereof.

13.3. The Data Importer shall:

- Certify the deletion of the Personal Data and all copies thereof to the Data Exporter;
- Provide documentation of the measures taken to ensure complete deletion or return, as applicable.

13.4. Until all Personal Data and copies thereof are either deleted or returned, the Data Importer shall continue to comply with the terms of these SANOFI BCR.

13.5. In case of local or national laws in the country of the Data Importer that prohibit the return or deletion of the transferred Personal Data or copies thereof, subject to such laws and practices meeting the requirements set forth in *Principle 11.1 (Assessment of Third Country laws and practices)*, the Data Importer shall:

- Inform the Data Exporter of such legal requirement;
- Warrant that it will continue to ensure compliance with these SANOFI BCR;
- Only process the data to the extent and for as long as required under the local or national laws of such Third Country.

Implement appropriate technical and organizational measures to limit the processing to what is legally required.

Section 2. Guarantees of bindingness, implementation & enforcement

14. Binding nature of these SANOFI BCR

14.1 These Binding Corporate Rules are legally binding for all SANOFI entities that have formally agreed to adhere to them. This binding commitment applies not only to these entities but also to all their Employees, who must comply with these rules in the course of their professional activities.

15. Cooperation with Data Protection Authorities

15.1 SANOFI cooperates fully with Data Protection Authorities and follows SANOFI's Privacy Rules. SANOFI regularly reviews decisions and guidance from these authorities to ensure compliance with these Binding Corporate Rules. This includes guidance from the European Data Protection Board (EDPB), the EU body that oversees data protection across Europe.

15.2 When Data Protection Authorities investigate or audit SANOFI, all SANOFI entities work together to provide complete cooperation. This means sharing all necessary information about how Personal Data is handled, including results from internal audits, whenever requested. Sanofi welcomes these audits and inspections, including visits to its facilities, as they help ensure proper data privacy practices.

15.3 If SANOFI disagrees with an official decision from a Data Protection Authority, it can challenge that decision in the courts of the relevant country under applicable laws. Any disputes about how Data Protection Authorities supervise these Binding Corporate Rules are resolved by the courts in the EU country where the authority is located, under that country's Privacy Laws.

16. Data Subject complaints

16.1 If individuals believe their rights have been violated or their requests regarding personal data have been denied, they can file a complaint against SANOFI. Complaints must be submitted in writing online via the webform at <https://www.sanofi.com/en/data-protection-contact>, or by mail at: EBI - Data Privacy Office, 46 Avenue de la Grande Armée 75017 Paris, France.

16.2 SANOFI acknowledges all complaints within five (5) working days and responds within one (1) month of receipt. For complex cases, this period may be extended by up to two (2) additional months, and individuals will be notified with a clear explanation. The complaint is first reviewed by the local data protection team and, if unresolved, escalated to SANOFI's Chief Data Privacy Officer. After investigation, SANOFI either takes corrective action or provides a detailed explanation.

16.3 Individuals retain the right to escalate matters, regardless of whether they have used or

completed SANOFI's internal procedure. This includes the right to:

- Lodge a complaint with relevant Data Protection Authorities (See [Third Party rights](#)).
- Bring legal action before competent courts (See [Third Party rights](#)).
- Seek judicial remedies, redress, and compensation for damages suffered (See [Right to judicial, remedies & compensation](#)).

- 16.4 These rights are available at any time and are not dependent on the Data Subject having used SANOFI's complaint handling process beforehand.

17. SANOFI BCR Update Procedure

- 17.1 SANOFI may update these Binding Corporate Rules at any time to reflect changes in Privacy Laws, regulatory guidance, or the SANOFI Group structure, while maintaining the same level of protection and binding commitments.
- 17.2 All updates are published on SANOFI's website at www.sanofi.com.
- 17.3 SANOFI maintains a detailed record of all modifications, including dates and descriptions of changes.
- 17.4 SANOFI reports all updates to the Lead Data Protection Authority annually and seeks prior approval for material changes.
- 17.5 Any new SANOFI entity must formally commit to these rules before receiving personal data transfers.

18. Accessibility of these SANOFI BCR

- 18.1 These SANOFI BCR are publicly available on SANOFI's website : www.sanofi.com
- 18.2 All individuals whose Personal Data are processed under these SANOFI BCR shall be provided with information on their rights as third-party beneficiaries, with regard to the processing of their Personal Data, and on the means to exercise those rights.
- 18.3 Individuals may also obtain a complete copy of these SANOFI BCR upon request.

19. Conflict of Law

- 19.1 The principles defined in these SANOFI BCRs constitute the minimum data protection standard applicable to all SANOFI BCR Members, regardless of their geographical location, for all Personal Data transfers within the scope of these SANOFI BCRs. Where local Applicable Privacy Laws conflict with these SANOFI BCRs, the SANOFI BCR Member must always apply the highest level of protection for Data Subjects, unless legally impossible. In all cases of conflict, the SANOFI BCR Member must promptly inform the Chief Privacy Officer and adhere to the additional requirements specified in [Principle 11](#).

20. Government requests for disclosure of Personal Data

- 20.1 When government authorities issue a Personal Data Disclosure Request seeking access to Personal Data, SANOFI follows a comprehensive procedure to ensure any disclosure remains strictly necessary and proportionate. This applies when SANOFI receives legally binding requests, becomes aware of direct or indirect access by authorities, or learns about such requests received by service providers.
- 20.2 If a SANOFI BCR Member acting as Data Importer receives a Personal Data Disclosure Request, it immediately informs the Data Privacy Office, the Data Exporter and, where possible, the affected individuals. If local laws prohibit notification, SANOFI documents its efforts to obtain permission for such notification. Each request undergoes thorough legal assessment by the local Legal Department and data protection specialists to ensure compliance with applicable laws and these rules.
- 20.3 SANOFI will never transfer personal data to government authorities—such as law enforcement or state security bodies—in a massive, disproportionate, or indiscriminate manner that goes beyond what is necessary in a democratic society. Any disclosure must be strictly limited to what is legally required and proportionate to the legitimate objective

pursued.

Section 3. Third Party Beneficiary Rights

21. Third Party rights

- 21.1 Data Subjects whose Personal Data is processed in the EEA by a SANOFI BCR Member acting as a Data Controller (*i.e.*, the Data Exporter) and is transferred to a SANOFI BCR Member located in a Third Country under these SANOFI BCR (*i.e.*, the Data Importer) may enforce these SANOFI BCR as Third-Party beneficiaries.
- 21.2 These rights do not extend to those elements of these SANOFI BCR pertaining to internal mechanisms implemented within SANOFI Group.
- 21.3 Data Subjects are entitled to enforce the following rights under these SANOFI BCR :
- The right to enforce these SANOFI BCR as Third-Party beneficiaries, including their right to invoke this third-party beneficiary status itself;
 - All data protection and privacy principles and lawfulness or processing requirements as set out in [Section 1.](#) of these SANOFI BCR;
 - Security measures and Personal Data Breach notification obligations ([Section 1.5](#));
 - Restrictions on onward transfers to Third Parties outside the SANOFI Group ([Section 1. ,10.](#));
 - Transparency and easy access to these SANOFI BCR (See [Accessibility of these SANOFI BCR](#));
 - SANOFI's obligations in case local laws and practices affect compliance with these SANOFI BCR or in case of a government access request ([0,11](#));
 - SANOFI's cooperation duties with the Competent Data Protection Authorities (See [Cooperation with Data Protection Authorities](#));
 - Rights of information, access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, and the right not to be subject to decisions based solely on automated processing, including profiling, the right to complain through the SANOFI's internal complaint process ([Section 1. ,9](#));
 - The right to be informed about any update of these SANOFI BCR and of the list of SANOFI BCR Members without undue delay (See [SANOFI BCR Update Procedure](#)).
 - The right to lodge a complaint in accordance with the Complaint Handling Procedure (see [Right to judicial, remedies & compensation](#)) and may also lodge a complaint with the Lead Data Protection Authority, the Competent Data Protection Authority or with a Data Protection Authority in the jurisdiction of their habitual residence, or place of work, or place of alleged infringement;
 - The right to judicial remedy and redress if a Data Subjects' rights under these SANOFI BCR have been infringed as a result of their Personal Data processed in breach of these SANOFI BCR (See [Right to judicial, remedies & compensation](#));
 - The right to compensation where Data Subjects who have suffered material or non-material damage as a result of an infringement of these SANOFI BCR have the right to receive compensation from SANOFI (See [Right to judicial, remedies & compensation](#));
 - The right to bring proceedings to enforce compliance with these SANOFI BCR before the competent courts of the EEA Member State (either the jurisdiction where the Data Controller is established), where the Lead Data Protection Authority or where the Data Subject has his/her habitual residence (See [Right to judicial, remedies & compensation](#));
 - The right to representation granted to Data Subjects to mandate a not-for-profit, organization or association, which has been properly constituted in accordance with the EU Law.

The detailed procedures for exercising these Data Subject's rights, including complaint handling, judicial remedies and compensation, are specified in [Section 3. Right to judicial, remedies & compensation](#).

- 21.4 Any Third-Party Rights requests should be sent to the SANOFI BCR Member through the

Data Subject Request form and will be managed by the competent Privacy Officer and Business Operational Team.

- 21.5 The relevant SANOFI BCR Member must promptly inform the Data Subject of the outcome of their request, and no later than one (1) month after receiving it. This notification should include, if applicable, the reasons for not taking action and the options for lodging a complaint with the Competent Data Protection Authority or seeking a judicial remedy. The one (1) month period may be extended by an additional two (2) months if necessary, considering the complexity and volume of requests.
- 21.6 The Competent Privacy Officer must notify the Data Subject of any such extension within one month of receiving the request, along with the reasons for the delay.
- 21.7 All communications, actions, and information provided in response to a Data Subject request shall be supplied at no cost. If the Data Subject's requests are clearly unfounded or excessive, especially due to their repetitive nature, the SANOFI BCR Member concerned may either:
- Charge a reasonable fee based on the administrative costs of providing the information or communication or taking the requested action, or
 - Refuse to fulfill the request.
- 21.8 The SANOFI BCR Member concerned must demonstrate that the request is manifestly unfounded or excessive.

22. Right to judicial, remedies & compensation

- 22.1 This section defines the framework and mechanisms for enforcing the Third Party rights as described in [Section 3. Third Party rights](#). It outlines the various remedies available to Data Subjects and enforcement mechanisms designed to ensure effective protection of Data Subjects' rights while establishing clear liability principles within the SANOFI Group.
- 22.2 *Jurisdiction and liability.* If a Data Importer violates these SANOFI BCR, individuals may bring proceedings against SANOFI before the competent courts or other judicial authorities including competent Data Protection authority in the EEA and the Lead Data Protection Authority where :
- The SANOFI BCR Member has an establishment,
 - The individual has his or her habitual residence, or place of work, or place of alleged infringement,
 - The Lead Data Protection Authority is located,
 - Individuals shall have the rights and remedies against the relevant Liable Sanofi BCR Member as if the violation had been caused by the latter in France, regardless of whether the actual violation was committed by the Data Importer or Data Exporter.
- 22.3 *Compensation.* Data Subjects may, at any time, seek compensation from the relevant Liable SANOFI BCR Member for any material or non-material damage suffered as a result of a breach of these SANOFI BCR, as determined by a court or other competent authority.
- 22.4 *Burden of proof.* If a Data Subject can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of a breach of these SANOFI BCR, the burden of proof shall rest with the Liable SANOFI BCR Member. The Liable SANOFI BCR Member must demonstrate that the SANOFI BCR Member outside of the EEA was not responsible for the breach giving rise to those damages, or that no such breach took place.
- 22.5 If the relevant Liable BCR Member provides such proof, it shall not be held liable or responsible for the damage claimed by the Data Subject.

These SANOFI BCR shall be effective upon approval by the Lead Data Protection Authority and be applicable to the SANOFI Affiliates upon signing the BCR Acceptation Agreement.

No Personal Data shall be transferred to a SANOFI Affiliate unless it is subject to these SANOFI BCR and SANOFI Transfer Framework. If a Data Importer is no longer bound by these SANOFI

BCR, it must immediately return or delete all Personal Data (including copies) transferred under these SANOFI BCR. However, the Data Importer may retain the transferred Personal Data if it offers legally binding commitments to safeguard the data in line with Chapter V of the GDPR.

PART III. APPENDICES

Appendix 1. Definitions

The content of these SANOFI BCR must be interpreted according to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (the "**GDPR**").

Words or expressions with a capital letter shall have the meaning assigned to them within the GDPR, Recommendations 1/2022 on the Application for Approval and the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of the EDPB ("**EDPB Recommendations 1/2022**"). In case of contradiction, the definitions of the GDPR shall prevail.

For the purpose of SANOFI BCR, the following terms shall have the meaning assigned to them as follows:

<i>Applicable Privacy Laws</i>	Personal Data protection laws, rules and regulations that provide at least the level of protection guaranteed by the EU Law applicable to the Processing Activities as amended from time to time. In case of transfers to SANOFI BCR Members established in Third Countries, the Personal Data Protection laws of the Data Exporter (including EU Laws where the Data Exporter is subject to it) shall be deemed applicable to the transferred Personal Data.
<i>BCR Acceptation Agreement</i>	A SANOFI intra-group agreement whereby SANOFI Affiliates undertake to be abided by these SANOFI Binding Corporate Rules.
<i>Business Operational Team</i>	SANOFI Employee(s), Temporary Staff and External Staff who shall comply with the Privacy Processes in accordance with SANOFI Privacy Rules including the relevant Privacy Officer's instructions.
<i>Business Process Owner</i>	Any SANOFI Employee who is in charge of projects, assets (e.g., software, hardware, systems, etc.) or activities that involve the processing of Personal Data in the context of their professional mission on behalf of one or several functions, business units (BU), countries and/or SANOFI Affiliate for one or several functions, business units or countries.
<i>Competent Data Protection Authority</i>	The Data Protection Authority in the European Economic Area (EEA) having jurisdiction to supervise a SANOFI BCR's Member processing of Personal Data within the scope of these SANOFI BCR, in accordance with EU Law.
<i>Data Controller</i>	The natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
<i>Data Exporter</i>	Any SANOFI BCR Member, regardless of its geographical location, that within the material scope of these SANOFI BCR, transfers Personal Data to another SANOFI BCR Member acting as a Data Importer. This definition includes, but is not limited to, SANOFI BCR Members established in the European Economic Area (EEA) transferring Personal Data to SANOFI BCR Members outside the EEA. It also covers Onward Transfers of Personal Data.

Data Importer	Any SANOFI BCR Member that, within the material scope of these SANOFI BCR, receives Personal Data from another SANOFI BCR Member acting as a Data Exporter. Under the EU Law, this definition refers to SANOFI BCR Members established outside the European Economic Area (EEA). For the purposes of SANOFI's internal data protection framework, by convention between SANOFI BCR Members, the term also covers any SANOFI BCR Member that receives Personal Data from another SANOFI BCR Member regardless of whether either entity is established within or outside the EEA.
Data Privacy Office	The team composed of Privacy Officers, the Privacy Legal Advisory Team and the Privacy Operations Team under the supervision of the Chief Privacy Officer, charged within SANOFI to (i) inform and advise SANOFI and its employees at group level of their legal obligations pertaining to Applicable Privacy Laws, (ii) monitor SANOFI compliance with Applicable Privacy Laws and SANOFI Privacy Rules and (iii) coordinate the network of Local Privacy Officers (LPO) and Functional Privacy Officers (FPO).
Data Processor	A natural or legal person (e.g., SANOFI Affiliate), public authority, agency, or other body that processes Personal Data on behalf of the Data Controller.
Data Protection Authority	A public entity vested with the authority for monitoring and enforcing data protection and privacy laws in its country, region, state or jurisdiction.
Data Subject(s)	Identified or identifiable natural person to whom the Personal Data that are being processed by SANOFI relate; an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.
Data Subject Request	A request made by a Data Subject who seeks to exercise Data Subject Rights.
Data Subject Rights	The legal rights granted by the EU Law to Data Subjects and which they can exercise towards the Data Controller, Data Processor or Data Exporter, Data Importer, Recipient.
Employee	Any SANOFI employee, whether full time or part time, temporary or trainee and any other employee category according to local regulation. Solely for the purposes of this procedure, the term <i>Employee</i> shall also include independent/external contractors hired by a SANOFI Affiliate, which shall not be interpreted as SANOFI being their employer, and SANOFI's Employee.
European Economic Area (EEA)	The geographical zone that includes the Member States of the European Union as well as the countries of the European Free Trade Association (EFTA).
EU Law	The General Data Protection Regulation ((EU) 2016/679) (the "GDPR") and, as applicable, the local and national laws relating to data protection and the processing of Personal Data and implementing the GDPR of a relevant EEA Member State.

Health Personal Data	Any information related to a Data Subject's physical or mental health whether or not pseudonymized. This includes data about medical conditions, diseases, treatments, medications, medical history, laboratory test results, genetic information, and any other data that is collected during the process of healthcare delivery, including in the context of clinical trials and studies. Health Personal data can also encompass lifestyle information, such as diet, exercise, and habits, as well as data from wearable devices or health apps.
Joint Controller	A Data Controller which determines the purpose and means of a Processing Activity with one or several other Data Controllers and whose roles and responsibilities are governed by a joint controllers agreement.
Lead Data Protection Authority	The French Data Protection Authority designated by the SANOFI Group as its lead authority under the GDPR. It is the Commission Nationale de l'Informatique et des Libertés (CNIL).
Liable(s) SANOFI BCR Member	Means SANOFI WINTHROP INDUSTRIE or SANOFI-AVENTIS RECHERCHE ET DEVELOPPEMENT, a company established within the European Union, which accepts responsibility, within the material scope of these SANOFI BCR as defined in Appendix 2 or any breaches of these SANOFI BCR committed by non-EU SANOFI BCR Member(s) and respectively undertake to take relevant steps for the remediation of such breaches and to pay compensation for any resulting damages on behalf of the non-EU SANOFI BCR Member in breach of these binding corporate rules.
Onward Transfer	A subsequent transfer of Personal Data initially received by a SANOFI BCR Member (Acting as Data Importer) to another SANOFI BCR Member to a Third Party, located in another country. This includes: • Transfers between SANOFI BCR Members located outside the EEA; • Transfers from a SANOFI BCR Member outside the EEA to a Third Party.
Personal Data	Any information processed by or on behalf of SANOFI relating to an identified or identifiable Data Subject (including but not limited to name and surname, contact details, social security number, financial information, medical data and Health Personal Data, professional education etc.). A Data Subject may be identified or identifiable indirectly in particular (i) by reference to an identifier such as an identification number, a patient number, a pseudonym, an online identifier or (ii) through the combination of several data (e.g., gender, date of birth and address) or (iii) by using factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.
Personal Data Breach	Means any incident resulting from a breach of security or confidentiality leading to the accidental or unlawful destruction, loss, alteration, theft, unauthorized disclosure of or unauthorized access to Personal Data and which may entail the obligation to send a specific notification to Competent Data Protection Authorities and communication to affected Data Subjects, where applicable.
Personal Data Disclosure Request	Any access request made by a public authority under the laws of the country of destination, or of another Third Country, for disclosure of Personal Data processed by SANOFI.

<i>Personal Data Processing Operation(s)</i>	Any operation performed on Personal Data such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
<i>Privacy Agreement</i>	Any contract, contract appendix or set of contractual clauses executed between one or several SANOFI Affiliate(s) with one or several Third Parties, specifically governing Processing Activity in accordance with Applicable Privacy Laws (including but not limited to Data Processing Agreements between a Data Controller and a Data Processor, joint-controllers agreement and independent Data Controllers agreement).
<i>Privacy Management System</i>	The digital platform used by the members of the Data Privacy Office to manage certain aspects of compliance with Privacy principles, including Privacy Processes.
<i>Privacy Officer</i>	A person who has been nominated by the Chief Privacy Officer as being responsible for the management of the privacy program and compliance at functional, regional or local level.
<i>Privacy Processes</i>	All processes included in the Global Privacy Operating Procedure describing the actions implemented by SANOFI to ensure compliance with the obligations arising from the Applicable Privacy Laws.
<i>Privacy Risk Assessment</i>	A SANOFI internal assessment to be carried out for a project, to evaluate the risks associated to the Processing Activity, to advise the Business Process Owner on the measures to be implemented to ensure an adequate protection of Personal Data and to document projects conducted in connection with a Processing Activity contained in SANOFI's Register(s).
<i>Processing Activity</i>	A specific SANOFI business activity carried out for a determined purpose or an ensemble of consistent purposes, that involves or requires one or several Personal Data Processing Operations and which shall be registered in the Register(s) of Processing Activities and subject to a Privacy Risk Assessment.
<i>Recipient</i>	A natural or legal person (e.g., a SANOFI Affiliate), public authority, agency or any other body to whom Personal Data are disclosed.
<i>Register(s) of Processing Activities</i>	Formal registers maintained by the Privacy Operations Team/Privacy Office in the Privacy Management System detailing all the Processing Activities performed by SANOFI allowing SANOFI to keep track and stay accountable regarding compliance with the EU Law. Registers of Processing Activities are implemented at : • A Global Business Unit (GBU) level, Global Function (GF) level in the <i>Register of Master Processing Activities (MRoPA)</i> • Geographical region level or country level (individual or Multi Country Organization) in the <i>Register of Local Processing Activities (LROPA)</i>.
<i>SANOFI Affiliate(s)</i>	Any legal entity which, directly or indirectly, controls, is controlled or is under common control of the SANOFI Parent Company. In relation to a legal entity, the term "control" means the direct or indirect ownership of more than fifty percent (50%) of the equity of such legal entity having the power to vote on or vote on or direct the affairs of the entity or direct the affairs of such legal entity.

<i>SANOFI BCR Member</i>	Any SANOFI Affiliate which (i) undertakes to implement the principles, rules and provisions set out in these SANOFI BCR (ii) expressly accepts to be bound by the entirety of the terms of these SANOFI BCR (iii) which duly executed the BCR Acceptation Agreement.
<i>SANOFI Group</i>	The group of companies comprising SANOFI Affiliates.
<i>SANOFI Parent Company</i>	The French corporation registered with the Paris Companies Registry under number RCS Paris 395 030 844.
<i>SANOFI Privacy Rules</i>	The policies, practices, guidelines, recommendations and advice adopted by and issued within the SANOFI Group designed to safeguard Personal Data that the company collects, processes, stores, and transmits. This includes notably these SANOFI BCR, the Global Privacy Policy and the Privacy Global Operating Procedure.
<i>SANOFI Transfer Framework</i>	The combination of these SANOFI BCR as well the intra-group data transfer agreement and the executed declarations of accession and any other document adopted or agreement entered into by SANOFI for the purpose of managing Personal Data transfers in compliance with Applicable Privacy Laws.
<i>Sensitive Personal Data</i>	The notion of Sensitive Personal Data, which may vary across countries, shall at a minimum, include information that relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, Health Personal Data, or data concerning a natural person's sex life or sexual orientation for the purpose of uniquely identifying a natural person, criminal convictions and offences.
<i>Third Country</i>	Any country that is not a member of the European Union or the European Economic Area.
<i>Third Party</i>	A natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, Data Processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorized to process Personal Data.

Appendix 2. Material scope

These SANOFI BCR provide a framework for the transfer of Personal Data between SANOFI BCR Members.

This document sets out the material scope of these SANOFI BCR. It specifies the Personal Data transfers or set of transfers, including the nature and categories of Personal Data, the type of Processing and its purposes, the types of Data Subjects affected.

1. Managing People and Culture

Who transfers the Personal Data described in this section ?	Every SANOFI BCR Member inside of the European Economic Area (EEA) may transfer the Personal Data that they control described in this section to every other SANOFI BCR Member inside and outside of the EEA. Every BCR Member outside of the EEA may also transfer the Personal Data that they control described in this section to every SANOFI BCR Member inside and outside of the EEA.
Who receives this Personal Data ?	Every SANOFI BCR Member outside of the EEA may receive the Personal Data described in this section which is sent to them by other Sanofi BCR Members inside and outside of the EEA. Every SANOFI BCR Member inside of the EEA may also receive the Personal Data described in this section which is sent to them by other SANOFI BCR Members inside and outside of the EEA.
Who are the types of individuals whose Personal Data are transferred ?	SANOFI Employees Job applicants
Which is the Liable SANOFI BCR Member ?	SANOFI WINTHROP INDUSTRIE
What categories of Personal Data are transferred ?	• Identification data – name, gender, photograph, date of birth, employee IDs. • Contact details – home and business address, telephone/email addresses, emergency contact details. • Employment details – job title/position, office location, employment contract, performance and disciplinary records, grievance procedures, sickness/holiday records. • Professional life data – training of past and current employment • Location data – geographical location of Data Subjects such as badges, geolocation data, travel information, meeting rooms bookings, flex office, office facilities • Background information – academic/professional qualifications, education, CV/résumé • National identifiers – national ID/passport, immigration/visa status, social security numbers. • Family situation – spouse and dependent information, marital status • Financial information – banking details, tax information, withholdings, salary, benefits, expenses, company allowances, stock and equity grants • IT information – information required to provide access to SANOFI's IT systems and networks such as IP addresses, log files and login information • Any other information provided voluntarily by Employees where justified and in accordance with Applicable Privacy Laws • Statistical information about SANOFI Employees • Background checks (such as criminal records) where justified and in accordance with Applicable Privacy Laws • Personal Health Data – <i>when work related</i>
What categories of Sensitive Personal Data (if any) are transferred ?	As a general rule, SANOFI does not transfer any Sensitive Personal Data relating to its Employees unless it is required to do so under Applicable Privacy Laws. In such a case, SANOFI may exceptionally transfer some information about: • An Employee's racial/ethnic origin

	• Religion • Gender and disabilities for the purposes of equal opportunities monitoring, to comply with anti-discrimination laws and for government reporting obligations; or • An Employee's physical or mental condition to provide work-related accommodations, health and insurance benefits (e.g., manage absences from work)
Why is this Personal Data transferred and how will it be used ?	SANOFI may transfer this Personal Data within the group in order to manage human resources at a group level, as well as for other processing activities such as compliance with Applicable Privacy Laws and regulations, training/development, IT services/security, audit and necessary investigations, tax and accounting, and general business management. In particular, the Personal Data may be used for the following purposes: - Recruitment - Talent management and organizational development (e.g., resource optimization, etc.) - Payroll, wages and salaries, salary market analysis, bonuses, equity grants (e.g., for stock and benefits plans administration) - Administration of healthcare, compensation, incentives programs and other benefits - Work-related injury and illness, absences, including the management of employee health and safety, and disabilities - Career planning, appraisals and performance management - International mobility (e.g., relocation) - Training/development, e-learning - Office management and employee support services (e.g., mobile phones, computers) - Business travel management and expense reimbursement - Emergency business continuity procedure - Management of company car fleet - IT support services and IT security/management - Telephone recordings for SANOFI Employee trainings and quality of service - Accounting, financial planning, internal audit, internal surveys and statistics - Disciplinary matters, internal investigations, anonymous hotline (e.g., whistleblowing) - To help SANOFI conduct its business more effectively and efficiently (e.g., for general HR resourcing on a global level) - Complying with legal or regulatory obligations and responding to requests from administrative or judicial authorities - Ensuring the physical security of people, of Sanofi's property and assets (e.g., access control, building entry/exit) - Managing corporate governance and compliance obligations (e.g., audit, delegations of authority/power, insiders lists, conflict of interests) - Evaluating and conducting business transactions and operations (e.g., sales, procurement, agreements) - Carrying out external and internal communication for events

<i>Where is this Personal Data processed ?</i>	The Personal Data described in this section may be processed in every territory where SANOFI BCR Members or their internal or external Data Processors are located.
<i>On what legal basis(es) is the Personal Data processed ?</i>	The Processing of Personal Data is necessary based on: - Performance of a contract (<i>i.e.</i>, employment contract and any other relevant contract) - Compliance with legal obligations (in particular labor law obligations) - SANOFI's legitimate interests - SANOFI Employee prior consent in limited cases and where SANOFI Employees have clearly expressed their approval of SANOFI's processing of their Personal Data

2. Health vigilance systems

<i>Who transfers the Personal Data described in this section ?</i>	Every SANOFI BCR Member inside of the European Economic Area (EEA) may transfer the Personal Data that they control described in this section to every other SANOFI BCR Member inside and outside of the EEA. Every BCR Member outside of the EEA may also transfer the Personal Data that they control described in this section to every SANOFI BCR Member inside and outside of the EEA.
<i>Who receives this Personal Data ?</i>	Every SANOFI BCR Member outside of the EEA may receive the Personal Data described in this section which is sent to them by other Sanofi BCR Members inside and outside of the EEA. Every SANOFI BCR Member inside of the EEA may also receive the Personal Data described in this section which is sent to them by other SANOFI BCR Members inside and outside of the EEA.
<i>Which is the Liable SANOFI BCR Member ?</i>	SANOFI-AVENTIS RECHERCHE ET DEVELOPPEMENT
<i>Who are the types of individuals whose Personal Data are transferred ?</i>	Person exposed to an adverse sanitary event Adverse sanitary events reporters (i.e., patient exposed to the adverse sanitary events patient relative, Health Care Professionals, member of an association, a member of health authority ...) Health Care Professionals (HCPs) (i.e., who may provide any clarifications)
<i>What categories of Personal Data are transferred ?</i>	• Identification data – name, gender, photograph, date of birth, age, identification number (e.g., numeric or alphabetical code) • Contact details – postal address, telephone/email address • Health Personal Data – treatments administered, examination results, nature of the adverse event or events, personal or family history, illnesses or associated events, risk factors
<i>What categories of Sensitive Personal Data (if any) are transferred ?</i>	• Health Personal Data
<i>Why is this Personal Data transferred and how will it be used ?</i>	SANOFI may transfer Personal Data within the group in order to manage the following purposes: - Recording - Analysis - Monitoring - Documentation - Transmission to health authorities
<i>Where is this Personal Data processed ?</i>	The Personal Data described in this section may be processed in every territory where SANOFI BCR Members or their internal or external Data Processors are located.
<i>On what legal basis(es) is the Personal Data processed ?</i>	The Processing of Personal Data is necessary based on: - Compliance with legal obligations (by local or regional health vigilance mechanisms)

3. Clinical trial and studies, Real-World Evidence studies

Who transfers the Personal Data described in this section ?	Every SANOFI BCR Member inside of the European Economic Area (EEA) may transfer the Personal Data that they control described in this section to every other SANOFI BCR Member inside and outside of the EEA. Every BCR Member outside of the EEA may also transfer the Personal Data that they control described in this section to every SANOFI BCR Member inside and outside of the EEA.
Who receives this Personal Data ?	Every SANOFI BCR Member outside of the EEA may receive the Personal Data described in this section which is sent to them by other Sanofi BCR Members inside and outside of the EEA. Every SANOFI BCR Member inside of the EEA may also receive the Personal Data described in this section which is sent to them by other SANOFI BCR Members inside and outside of the EEA.
Which is the Liable SANOFI BCR Member ?	SANOFI-AVENTIS RECHERCHE ET DEVELOPPEMENT
Who are the types of individuals whose Personal Data are transferred ?	Patients (i.e., participants) Health Care Professionals (HCPs) involved in the clinical trial and study
What categories of Personal Data are transferred ?	• Identification data – name, gender, photograph, video, voice recording, date of birth, age, identification number (e.g., numeric or alphabetical code), ethnic origin • Contact details – postal address, telephone/email address • Health Personal Data – e.g., medical information, biological data, weight, height, personal or family antecedents, genetic data... • Family situation – • Background information – academic/professional qualifications, education • Financial information – banking details, reimbursement of expenses, amount of allowance & remuneration received • IT information – information required to provide access to IT systems and networks such as log files and login information
What categories of Sensitive Personal Data (if any) are transferred ?	• Health Personal Data • Sex life • Racial/ethnic origin
Why is this Personal Data transferred and how will it be used ?	SANOFI may transfer Personal Data within the group in order to manage the following purposes: - Assess the safety and efficacy of investigational medicinal products - To promote healthcare to comply with regulatory requirements; to market or to continue to market and to support reimbursement activities - Conduct disease driven study or clinical exploratory study such as assay validation methodology study, experimental medicine pharmacological or physiological models - Assess the safety and effectiveness of investigational post-marketed products conducted for the purpose of developing biological, scientific, or medical knowledge, and in which all procedures are performed and products used in a usual manner during routine medical practice

	- Personal Data will be processed through recording, analysis, monitoring, documentation, transmission and retention activities. The Personal Data processed will be compiled in a study Report (e.g., Clinical Study Report) for submission to health authorities)
<i>Where is this Personal Data processed ?</i>	The Personal Data described in this section may be processed in every territory where SANOFI BCR Members or their internal or external Data Processors are located.
<i>On what legal basis(es) is the Personal Data processed ?</i>	The Processing of Personal Data is necessary based on: - SANOFI's legitimate interests in the area of public health such as ensuring high standards of quality and safety of medicinal products or medical devices (art 9.2.i) GDPR) - When required by local regulations, another legal basis may justify the Processing of Personal Data (i.e., the consent) - Compliance with legal obligation (i.e., safety)

Appendix 3. GDPR Provisions

Article 37, GDPR

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:
 - (a) The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
 - (b) The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
 - (c) The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.
5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.
6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 39, GDPR

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:
 - (a) To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
 - (b) To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
 - (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
 - (d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Article 89(1), GDPR

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.