SERVIER

BINDING CORPORATE RULES (BCRS) FOR INTRA-GROUP TRANSFERS OF PERSONAL DATA

Table of Contents

1. INTRODUCTION

SERVIER is committed to ensure a high level of protection of Personal Data throughout the group and to comply with applicable laws and regulations regarding the Processing of the Personal Data of its employees, customers, suppliers and other business partners such as health professionals, medical sales representatives and pharmacists.

The adoption and the implementation of Binding Corporate Rules (BCRs) within the SERVIER Organization aims at regulating all intra-group cross-border transfers and, in particular, intra-group data transfers relating to Personal Data outside the EEA, in accordance with the provisions of Regulation (EU) 2016/679
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 (General Data Protection Regulation or "GDPR") and Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector as amended by Directive 2009/136/EC of 25 November 2009 (Directive on privacy and electronic communications or "E-Privacy Directive").

According to the GDPR, any transfer of Personal Data outside the EEA shall be framed by specific safeguards in order to ensure that the use of Personal Data made by the group is compliant with European data protection principles. In addition, it is worth underlying that BCRs are enshrined at the core of the GDPR, which explicitly recognizes this set of binding rules as an adequate safeguard to frame transfers of Personal Data outside the EEA.

SERVIER perceives these BCRs as an essential tool to effectively promote our culture on data protection within the SERVIER Organization. These BCRs will also foster data protection compliance and ease the management of Personal Data within the whole group. SERVIER and its Employees are responsible for protecting and respecting Personal Data that they process and to which they have access.

With regard to the scope of our BCRs, the Companies of SERVIER Organization which adhere to the BCRs and their Employees shall comply with the following provisions as well as with applicable local laws and regulations. SERVIER has set up an effective governance structure to manage such data protection obligations.

The BCRs will apply when the transfer of Personal Data is not otherwise permitted by Article 49 of the GDPR[1] and/or the applicable law and to any subsequent onward transfer that is not otherwise permitted by applicable law.

At local levels, each Local Data Controller will either have to sign the present BCRs, or will sign further a BCRs intra-group agreement (Appendix 4). In any case, the respective SERVIER Companies shall take all necessary steps to ensure compliance with the provisions of the BCRs. Compliance with these provisions and procedures will especially rely on data protection training programs of SERVIER's personnel and auditing activities.

[1] In accordance with Article 49 of the GDPR and applicable local law, in the absence of an adequacy decision pursuant to Article 45(3) or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of Personal Data to a third country or an international organization shall take place only on one of the following conditions:

- The Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;
- The transfer is necessary for the performance of a contract between the Data Subject and the Local Data Controller or the implementation of precontractual measures taken at the Data Subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Local Data Controller and another natural or legal person;
- The transfer is necessary for important reasons of public interest the transfer is necessary for the establishment, exercise or defence of legal claims;
- The transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving Consent;
- The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

Because of their wide scope in terms of data protection compliance, the use of the BCRs at local levels will without any doubt, ease the management of data protection compliance and will help to ensure that local representatives takes ownership of data protection.
Would a violation of the BCRs be established, any corrective measures (legal, technical or organizational) as well as any appropriate sanction (against the Local Data Controller and/ or a local Employee, if allowed under the respective local law) may be imposed on the recommendation of the Head Controller, the Global Data Protection Officer and the relevant Local Data Protection Officer(s) or Contact(s).

2. DEFINITIONS AND DATA PROTECTION PRINCIPLES

2.1. DEFINITIONS

The terms and expressions used in the BCRs and its appendices, which are written with a capital letter, shall have the meaning set out below, provided that these terms and expressions shall always be interpreted according to the GDPR and the E-Privacy Directive.

"**Applicable Data Protection Law**" shall mean the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to Personal Data protection with respect to the Processing of Personal Data applicable to a Data Controller located in any country where SERVIER is located and in which the Local Data Exporter is established. Local Data Protection Law applies to local processing activities as public order law in parallel with BCRs which constitute a contractual commitment for adhering companies. Any conflicts between Applicable Data Protraction Law and BCRs are meant to be handled as described in paragraph 7.2. below.

"Consent" of the Data Subject shall mean any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

"**Controller**" or "**Data Controller**" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

"**Data Subject**" shall mean an identified or identifiable natural person to whom Personal Data relates. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Data Transfer**" shall mean any transfer of Personal Data from a Company to another Company. A transfer can be carried out via any communication, copy, transfer or disclosure of Personal Data through a network, including remote access to a database or transfer from a medium to another, whatever the type of medium (for instance from a computer hard disk to a server).

"**EEA or European Economic Area**" shall mean the countries of the European Union and countries members of EFTA (European Free Trade Association).

"Employees" are all people which perform, or performed in the past, duties for the SERVIER Organization, in exchange for wages or a salary, according to an employment contract (where applicable or required by law) or any other assimilated agreement (such as internship agreement) and under a subordination relationship. This also includes directors, trainees, apprentices, contingent workers and assimilated status.

"**Genetic Data**" shall mean any personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

"**Global Data Protection Officer**" shall mean the senior level manager who is responsible, within the SERVIER Organization at a global level, for managing business awareness and compliance with Applicable Data Protection Law and SERVIER data protection policies, procedures and guidelines,

especially the BCRs. SERVIER's Global Data Protection Officer reports directly to or is part of the Management Board.

"**Head Controller**" shall mean SERVIER SAS, a French Société par Actions Simplifiée, having its principal offices at 50 rue Carnot, 92150 Suresnes, registered in the Commercial Registry of Nanterre under the number 324444991. The Head Controller, SERVIER SAS, is the company which manages operations the SERVIER Organization in Europe, and as such, alone or jointly with other SERVIER Companies, determines the purposes and means of the Processing of Personal Data within the Organization. The Head Controller shall have delegated data protection responsibilities for all of the Processing of Personal Data within the scope of the GDPR, be in charge of the application for formal BCR and of the relationships with the coordinating Data Protection Authorities.

"Health Professionals" shall mean any individual who provides preventive, curative, promotional or rehabilitative health care services in a systematic way to people, families or communities. Health professionals include physicians, dentists, pharmacists, pharmacy technicians, physician assistants, nurses, advanced practice registered nurses, surgeons, surgeon's assistant, athletic trainers, surgical technologist, midwives, dietitians, therapists, psychologists, chiropractors, clinical officers, social workers, phlebotomists, occupational therapists, optometrists, physical therapists, radiographers, radiotherapists, respiratory therapists, audiologists, speech pathologists, operating department practitioners, emergency medical technicians, paramedics, medical laboratory scientists. Health professionals have no contractual any other subordination relationship with SERVIER. They constitute the main recipients of SERVIER's marketing activity.

"**Leading Supervisory Authority**" shall mean the Commission Nationale de l'Informatique et des Libertés or the CNIL.

"**Local Data Controller**" shall mean the Company of the SERVIER Organization which alone or jointly with others, mainly the Head Controller, determines the purposes and means of the Processing of Personal Data within its scope of competence

"**Local Data Exporter**" shall mean the Company of the Organization which transfers the Personal Data outside its Company.

"**Local Data Importe**r" shall mean the Company of the SERVIER Organization which agrees to receive Personal Data from the Local Data Exporter for further Processing.

"Local Data Protection Officer" shall mean the person potentially designated within the SERVIER entity concerned in compliance with Article 37 of the GDPR, in order to inform and advise about applicable data protection rules, monitor compliance with these rules and any related applicable policy, cooperate and act as a point of contact with the Supervisory Authority.

"Local Data Protection Contact" means the person potentially designated within a SERVIER entity as a point of contact relating to data protection, where the requirement to appoint a DPO under the GDPR is not applicable.

Together "**Local Data Protection Officer or Contact**".

"Medical Sales Representatives" shall mean any individual working for SERVIER and selling on its behalf drugs, medicines and medical equipment to health professionals. Medical Sales Representatives may be or not SERVIER's employees.

"**Personal Data**" shall mean any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Personal Data Concerning Health" shall mean Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

"Personal Data Breach" shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"**Processing of Personal Data"** shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" shall mean a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Controller.

"Profiling" means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

"Pseudonymisation" means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

"**Recipient**" shall mean a natural or legal person, public authority, agency or another body to which the Personal Data are disclosed, whether a Third Party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry shall not be regarded as Recipients.

"**Records of Processing Activities**" shall mean the records of Processing activities implemented either by a Controller or a Processor in line with Article 30 of the GDPR.

"SERVIER Organization" or "**SERVIER**" shall mean SERVIER SAS , and any other company controlled by SERVIER SAS, with a company being considered as controlling another: (a) when it holds directly or indirectly a portion of the capital which provides the majority of the voting rights in general meetings of shareholders of this company; (b) when it holds solely the majority of the voting rights in this company by virtue of an agreement concluded with other partners or shareholders and which is not contrary to

the interest of the company; (c) when it determines de facto, by voting rights which it holds, the decisions in the general meetings of shareholders of this company; (d) when it is a partner or shareholder of this company and holds the power to nominate or to revoke the majority of members of the administrative, management or supervisory bodies or (e) in any event, when it holds, directly or indirectly, a portion of voting rights greater than 40% and when no other partner or shareholder holds directly or indirectly a portion which is greater than its own.

"**SERVIER Companies**" or "Company(ies)" shall mean all Companies part of the SERVIER Organization which have signed the present BCRs or the intra-group agreement (Appendix 4) in their capacity to be bound to the BCRs either as Data Exporters or as Data Importers.

"**Special Categories of Personal Data**" shall mean Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, Data Concerning Health or a natural person's sex life or sexual orientation.

"**Supervisory Authority**" shall mean an independent body which is in charge of: (i) monitoring the Processing of Personal Data within its jurisdiction (country, region or international organization) according to the GDPR and enforcing its application, (ii), providing advice to the competent bodies with regard to legislative and administrative measures relating to the protection of Data Subjects' rights with regard to Processing of Personal Data, (iii) promoting the awareness of Controllers of their obligations under the GDPR, (iv) provide information to any Data Subject concerning the exercise of their rights under the GDPR and, if appropriate, cooperate with the supervisory authorities in other Member States, (v) handling complaints lodged by Data Subjects with regard to the protection of their data protection rights and (vi) fulfil any other tasks related to the protection of Personal Data.

"**Third Party**" shall mean a natural or legal person, public authority, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the data.

2.2. DATA PROTECTION PRINCIPLES

Within the scope of the BCRs (see paragraph 4), any Data Transfer to a third country which does not ensure an adequate level of protection shall always comply with the following data protection principles, defined in specific paragraphs of the BCRs or in Appendix 1, in accordance with the provisions of the GDPR and the E-Privacy Directive.

- **Fairness and Transparency of the Processing:** Fairness requires that the Data Subject be informed of the existence of the Processing operation and its purposes. Any information and communication relating to the Processing of the Data Subjects' Personal Data shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

- **Lawfulness:** In order for Processing to be lawful, Personal Data should be processed on the basis of the consent of the Data Subject concerned or some other legitimate basis, laid down by law, either in the GDPR or in other Union or Member State law, including the necessity for compliance with the legal obligation to which the Controller is subject or the necessity 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.

- **Purpose limitation**: Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (see Appendix 1).

- **Data minimization**: Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and/or processed (see Appendix 1).

- **Limited storage periods**: Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are processed (see Appendix 1).

- **Data quality**: Personal Data shall be accurate and, where necessary, kept up to date (accuracy) (see Appendix 1).

- **Data protection by design**: it is necessary to implement, both at the time of the determination of the means for Processing and at the time of the Processing itself, appropriate technical and organizational measures (such as Pseudonymization), which are designed to implement data-protection principles (such as data minimization), in an effective manner and to integrate the necessary safeguards into the Processing (see Appendix 1).

- **Data protection by default**: it is necessary to 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 (see Appendix 1).

- **Lawful basis for Processing Personal Data and Processing Special Categories of Personal Data**: Personal Data and Special Categories of Personal Data shall only be processed under the conditions defined in the GDPR (see Appendix 1).

- **Security of Personal Data**: Appropriate technical and organizational measures shall be implemented to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of or access to and against all other unlawful forms of Processing (see paragraph 5.5 and Appendix 1).

- **Onward transfers to organizations not bound by BCRs:** when Personal Data is intended to be transferred to a non-SERVIER Company, adequate safeguards have to be implemented (se paragraph 5.6 and Appendix 1).

The Local Data Controller shall be responsible for, and be able to demonstrate compliance with the present data protection principles (**accountability**).

3. PURPOSE OF THE BCRs

The purpose of these BCRs is to ensure an adequate level of protection for transfers of Personal Data within the SERVIER Organization. SERVIER has decided to implement BCRs as part of the SERVIER data protection compliance program, as defined by the European regulations in order to (i) facilitate and improve international flows of Personal Data within SERVIER and (ii) put in place a global data protection governance.

4. SCOPE OF THE BCRs

4.1. GEOGRAPHICAL SCOPE

The present BCRs shall apply to the transfers of Personal Data between Companies of the SERVIER Organization established throughout the world and which have signed the present BCRs, or a BCRs intra-group agreement (Appendix 4). Appendix 2 includes a list of SERVIER Companies that are bound by the BCRs.

4.2. MATERIAL SCOPE

The nature and purposes of the Personal Data being transferred within the scope of the BCRs are detailed in Appendix 3.

5. EFFECTIVENESS OF THE BCRs

5.1. TRANSPARENCY AND RIGHT OF INFORMATION

To make the data Processing fair, Personal Data shall always be collected and processed in a transparent manner. Thus:

1. Data Subjects should be provided with the information as required by Articles 13 and 14 GDPR (as provided below), information on their third party beneficiary rights (as provided in Article 6.3 below) with regard to the Processing of their Personal Data and on the means to exercise those rights, the clause relating to the liability (as provided in article 6.4. below) and the clauses

relating to the data protection principles (as provided in Appendix 1). The information must be complete and not only summarized.

Every Data Subject has the right to have an easy access to the BCRs. Relevant parts of the BCRs will be published on the internet and on the intranet of the Company. In any case, the Data Subject shall always be able to obtain, upon request, a copy of the BCRs from the SERVIER relevant Local Data Protection Officer(s) or Contact(s).

2. Furthermore, some educational material shall be made available to the Data Subjects, with a view to clarify on the BCRs or any related matter, such as submitting an access request to their Personal Data (see paragraph 5.2) or submitting a claim (see paragraph 5.4).

3. Data Subjects are entitled to be informed of the Processing of their Personal Data. Consistent with this aim, relevant Local Data Protection Officer(s) or Contact(s), in coordination with the Global Data Protection Officer, shall provide, when appropriate, templates of information notices to every Local Data Controller within the SERVIER Organization.

4. Where, with regard to an existing Processing, a new purpose or a new category of Recipient arises, the appropriate information notice shall be consequently modified and the relevant Data Subjects shall be informed of such modification.

SERVIER Organization will provide a Data Subject with at least the following information, except where the Data Subject already has the information:

a. the identity and contact details of the Local Data Controller or of his representative, if any;;
b. the contact details of the Local Data Protection Officer or Contact;
c. the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;
d. the legitimate interests pursued by the Local Data Controller or by a Third Party (when the Processing is based on this ground);
e. the Recipients or categories of Recipients of the Personal Data, if any;
f. where applicable, the fact that the Local Data Controller intends to transfer Personal Data to a third country, the existence or absence of an adequacy decision by the European

Commission or the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;

g. the period for which the Personal Data will be stored (or the criteria used to determine that period);
h. the existence of the right to request from the Local Data Controller access to and rectification or erasure of Personal Data or restriction of Processing or to object to Processing as well as the right to data portability where such right is applicable;
i. where the Processing is based on the Data Subject's Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before withdrawal;
j. the right to lodge a complaint with a Supervisory Authority;
k. whether the provision of Personal Data is statutory or contractual as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
l. the existence of Automated Decision-making (if any), including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;
m. the intention to further process the Personal Data for a purpose other than for which it was collected;
n. from which source the Personal Data originates and if applicable whether it came from publicly accessible source (where Personal Data has not been obtained directly from the Data Subject).

Where the data has not been directly obtained from the Data Subjects, SERVIER will provide the relevant Data Subjects with the information above within a reasonable period after obtaining the Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Personal Data are processed; if the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or if a disclosure to another Recipient is envisaged, at the latest when the Personal Data are first disclosed.

However, according to Article 14(5) of the GDPR, which applies where the Personal Data have not been directly obtained from the Data Subjects, this disclosure of information to the Data Subject will

exceptionally not apply where the Data Subject already has the information, the provision of such information proves impossible or would involve a disproportionate effort, if obtaining or disclosure is expressly laid down by law to which the Data Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests or where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by law (including a statutory obligation of secrecy).

5.2. RIGHTS OF ACCESS, RECTIFICATION, ERASURE, RESTRICTION OF PROCESSING, TO OBJECT TO THE PROCESSING AND TO DATA PORTABILITY

1. **Every Data Subject has the right (after having established his identity) to:**

a. **Obtain from SERVIER without constraint, at reasonable intervals and without excessive delay or expense:**
   - confirmation as to whether or not Personal Data relating to the Data Subject is being processed;
   - if it is the case, information at least as to the purposes of the Processing, the categories of Personal Data concerned, the Recipients or categories of Recipients to whom the Personal Data is disclosed, where possible the envisaged period for which the Personal Data will be stored or if not possible the criteria used to determine that period, the existence of the right to request from SERVIER rectification or erasure of Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing, the right to lodge a complaint with a Supervisory Authority, any available information as to their source (where the Personal Data are not collected from the Data Subject); the existence of Automated Decision-making, including Profiling and, at least, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;
   - where Personal Data are transferred to a third country, information about the appropriate safeguards used for the Data Transfer;
   - communication to the Data Subject in an intelligible form of the Personal Data undergoing Processing;

b. **Obtain from SERVIER, without undue delay, the rectification of inaccurate Personal Data concerning him or her**. Taking into account the purposes of the Processing, the Data Subject has the right to have incomplete Personal Data completed, including by means of providing a supplementary statement;

c. **Obtain from SERVIER without undue delay, the erasure of Personal Data** concerning him or her where one of the following grounds applies: i) where the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; ii) where the Data Subject withdraws Consent on which the Processing is based and there is no other legal ground for the Processing and there are no overriding legitimate grounds for the Processing; iii) the Data Subject objects to the Processing in accordance with point g. below when there are no overriding legitimate grounds for the Processing or the Data Subject objects to the Processing for the purposes of direct marketing with point h. below; iv) the Personal Data has been unlawfully processed; v) the Personal Data has to be erased for compliance with a legal obligation to which SERVIER is subject; vi) the Personal Data has been collected in relation to the offer of information society services;

Where SERVIER has made the Personal Data processed public and is obliged to erase the Personal Data, SERVIER will take reasonable steps, including technical measures, to inform Controllers which are Processing the Personal Data that the Data Subject has requested the erasure by such Controllers of any links to, or copy or replication of, those Personal Data (taking account of available technology and the cost of implementation);

However, exceptions to this right to erasure apply i) when the Processing is necessary for exercising the right of freedom of expression and information; ii) for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; iii) for reasons of public interest in the area of public health; for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; for the establishment, exercise or defense of legal claims;

d. **Obtain from SERVIER restriction of Processing** where one of the following grounds applies: i) when the accuracy of the Personal Data is contested (for the period necessary to verify the accuracy of the data), ii) when the Processing is unlawful and the Data Subject requests the restriction of their use, iii) when SERVIER no longer needs the Personal Data for the purposes of the Processing but they are required by the Data Subject for the establishment, exercise or defense of legal claims and iv) when the Data Subject has objected to a Processing based on the legitimate interest of SERVIER (for the period necessary to verify whether the legitimate grounds of SERVIER override those of the Data Subjects if applicable Processing);

e. **Have SERVIER communicate to each Recipient to whom the Personal Data have been disclosed of any rectification, erasure or restriction carried out in compliance with (b), (c), (d)**, unless this proves impossible or involves a disproportionate effort. The Controller shall inform the Data Subject about those Recipients if the Data Subject requests it;

f. **Exercise his or her right to data portability** and obtain from SERVIER the right to receive the Personal Data concerning him or her, which he or she has provided to SERVIER, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from SERVIER, when the Processing is based on Consent or on a contract and the Processing is carried out by automated means;

g. **Object at any time on compelling legitimate grounds** relating to the Data Subject's particular situation to the Processing of Personal Data (based on the legitimate interest of SERVIER) relating to the Data Subject;

   According to the GDPR, the exercise of the foregoing rights may be subject to certain limitations, in particular Local Data Controllers may charge a reasonable fee or refuse to act on the requests that are manifestly unfounded or excessive, in particular because of their repetitive character;

h. **Object, at any time of the Processing, free of charge and without having to state legitimate grounds, to the Processing of Personal Data for the purposes of direct marketing** (including Profiling to the extent that it is related to such direct marketing).

2. In order to enable Data Subjects to exercise efficiently their rights, specific guidelines and procedures shall be in place within the SERVIER Organization, at local levels, to ensure the exercise of the rights specified above. In particular, SERVIER's Employees who collect, process or have access to Personal Data shall be trained to recognize a Data Subject's request for access, rectification, erasure, restriction, objection or portability. Each request shall be acknowledged and handled according to the local procedure in place.

3. A specific answer shall be given to the Data Subject within a reasonable period of time (i.e., no later than one month of receipt of the request. That period may be extended by two further months where necessary taking into account the complexity and number of the requests. SERVIER shall inform the Data Subject of any extension within one month of receipt of the request together with the reasons for the delay).

4. If the request is found legitimate, SERVIER shall take necessary steps to handle the matter in due time. If the request is denied, the Data Subject shall be informed in writing or by email about the reason for and the fact that the Data Subject may follow the internal complaint mechanism specified in paragraph 5.4.

5. Relevant Local Data Protection Officer(s) or Contact(s), in coordination with the Global Data Protection Officer, shall be available to both Local Data Controllers and Data Subjects to assist them in relation to Data Subjects' requests when necessary.

5.3. AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING

1. Subject to Applicable Data Protection Law, every Data Subject has the right not to be subject to a decision based solely on automated Processing, including Profiling, which produces legal effects concerning him or her or significantly affects him or her.

2. The above does not apply if the decision:
   - is necessary for entering into, or performance of, a contract between the Data Subject and SERVIER;

- is authorized by Union or national law to which SERVIER is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests;
- or is based on the Data Subject's explicit Consent.

5.4. INTERNAL COMPLAINT MECHANISM

1. If a Data Subject reasonably believes that there has been a violation of these BCRs or that the Data Subject's Personal Data is processed in a way that is incompatible with these BCRs, the Data Subject may lodge, in accordance with the **BCRs Complaint Procedure**, a complaint to obtain adequate correction measures and, where appropriate, adequate compensation (see paragraph 6.3). Therefore:

a. Specific guidelines and procedures shall be in place within the SERVIER Organization, at local level, to ensure the consistency of the complaint mechanism and to ensure sufficient information to be provided to the Data Subjects about these procedures. The complaints shall be dealt with by a clearly identified local department which benefits from an appropriate level of independence in the exercise of its functions (for instance, it is the Local Data Protection Officer or Contact). When a complaint is registered, it must be acknowledged and handled within a reasonable period of time (i.e., no later than one month of receipt of the request. That period may be extended by two further months where necessary taking into account the complexity and number of the requests. SERVIER shall inform the Data Subject of any extension within one month of receipt of the request together with the reasons for the delay).

b. If the SERVIER relevant Local Data Protection Officer(s) or Contact(s) fail to solve the claim at local level, the complaint handling mechanism shall allow escalating the problem to the Global Data Protection Officer who shall respond in the timeline indicated above. Each Local Data Controller and each Local Data Protection Officer or Contact shall regularly report to the Global Data Protection Officer about the complaints settled at local level.

c. All SERVIER's representatives and Employees shall, at local level, do their best efforts to help the Local Data Controller to settle a complaint.

d. All data protection complaints received by the relevant Local Data Protection Officer(s) or Contact(s) or any other contacted person shall be communicated to the relevant Local Data Protection Officer(s) or Contact(s) and the Global Data Protection Officer without any delay.

2. Each SERVIER Company shall make available on an online environment, especially on www.SERVIER.com, practical tools or procedures allowing Data Subjects to lodge their complaints, including at least one of the below:
    - Web link to complaint form
    - Email address
    - Telephone number
    - Postal address.

For the avoidance of doubt, it is understood that if the Data Subject is not satisfied by the replies of the Local Data Protection Officers or Contacts and ultimately, the Global Data Protection Officer or if the Data Subject prefers to bypass the available internal complaint mechanism, the Data Subject has the right to lodge a complaint before the relevant Supervisory Authority in the Member State of his habitual residence, place of work or place of the alleged infringement or before the competent court of the EU Member States (see paragraph 6.3).

Prior to referring a case to the relevant Supervisory Authority or competent jurisdiction, the Data Subject shall be informed of the possibility to solve a claim through the internal complaint mechanism described above and the **BCRs Complaint Procedure**.

5.5. SECURITY AND CONFIDENTIALITY / RELATIONSHIPS WITH PROCESSORS THAT ARE MEMBERS OF THE GROUP

5.5.1. General security and confidentiality principles

Ensuring that Personal Data is appropriately protected from Personal Data Breaches is a SERVIER priority. Thus:

1. Each Local Data Controller shall implement appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, taking into consideration the state-of-the-art technology and the cost of implementation, the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

   Furthermore, the implemented measures shall ensure (i) a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, such as including, where appropriate, the Pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

   Consequently, appropriate information security policies and procedures shall be designed and implemented within the SERVIER Organization to set up all appropriate physical and logistical measures. These policies and procedures shall be regularly audited (see paragraph 5.8).

2. Special Categories of Personal Data shall be processed with enhanced and specific security measures.

3. Access to Personal Data is limited to Recipients for the sole purpose of performing their professional duties. Disciplinary sanctions may occur if a SERVIER's Employee fails to comply with the appropriate information security policies and procedures.

5.5.2. Relationships with Processors that are members of the SERVIER Organization

Where a Local Data Controller requests that another Company of SERVIER undertakes Processing of Personal Data on its behalf, the following safeguards shall be followed:

1. Where the Processing is carried out, the Local Data Controller shall choose a Processor providing sufficient guarantees to implement appropriate technical and organizational security measures governing the Processing to be carried out, and must ensure compliance with those measures. Any Company of SERVIER which is bound by the BCRs by signing the present BCRs as of the date hereof or the signature of the BCRs intra-group agreement in Appendix 4 undertakes to provide those sufficient guarantees and to comply with all safeguards contained herein when acting as a Processor on behalf of a Local Data Controller.

2. The Local Data Controller may decide to use another SERVIER entity acting as a Processor and/or sub-processor for the purpose of Processing, the type of Personal Data and categories of Data Subjects as described in Appendix 3 of the BCRs, for the subject matter and duration instructed by the Local Data Controller and in compliance with the provisions listed below.

3. The appointed Company of SERVIER (Processor and/or sub-processor) undertakes:
   - To process the Personal Data only on documented instructions from the Local Data Controller; unless the Processor is required to do so by law to which the Processor is subject, in which case the Processor shall promptly notify the Local Data Controller (unless prohibited by law or important grounds of public interest)
   - To ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
   - To implement technical and organizational security measures to sufficiently protect the Personal Data against any accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access;
   - To respect the conditions for engaging another Processor (see below);
   - To assist the Local Data Controller, taking into account the nature of the Processing, by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Local Data Controller's obligation to respond to requests for exercising the Data Subject's rights as indicated in paragraph 5.2 above;
   - To assist the Local Data Controller in ensuring compliance with its obligations as regards the security of Personal Data, the notification of a Personal Data Breach, the data protection impact assessment and the prior consultation of the local DPA (where necessary);

- At the choice of the Local Data Controller, to delete or return all the Personal Data to the Local Data Controller after the end of the provision of services relating to Processing, and deletes existing copies unless national law requires storage of the Personal Data;
- To make available to the Data Controller all information necessary to demonstrate compliance with these obligations and allow and contribute to audits of its Processing activities including inspections, conducted by the Local Data Controller or another auditor mandated by the Local Data Controller;
- To inform the Local Data Controller if in this opinion an instruction infringes the applicable Data Protection provisions;
- To implement procedures for managing Personal Data breaches and to notify the Local Data Controller without undue delay after becoming aware of a Personal Data Breach;
- Not to disclose Personal Data to any Third Party outside the SERVIER Organization without the prior explicit Consent of the Local Data Controller (see also paragraph 5.6 below regarding Data Transfers outside of the SERVIER Organization). In case of Consented disclosure, the same data protection obligations as set out above will be imposed by the appointed Company of SERVIER (Processor) on that other Processor by way of a contract. Where that other Processor fails to fulfil its data protection obligations, the appointed Company of SERVIER (Processor) shall remain fully liable to the Local Data Controller for the performance of that other Processor's obligations.

4. The Local Data Controller agrees that a SERVIER Company acting as Processor uses another Company within the SERVIER Organization for sub-Processing. In this case, the initial Processor undertakes to inform the Local Data Controller of any intended changes concerning the addition or replacement of other Processors, thereby giving the Local Data Controller the opportunity to object to such change.

5. If the Processor determines the purposes and means of Processing, the Processor is considered to be a Controller in respect of that Processing.

6. The appointed Company of SERVIER (Processor) must maintain a Record of Processing Activities carried out on behalf of the Local Data Controller.

7. The appointed Company of SERVIER (Processor) will be held liable for the damage caused by Processing where it has not complied with obligations of the GDPR specifically directed to Processors or where it has acted outside or contrary to lawful instructions of the Local Data Controller (except if it proves that it is not in any way responsible for the event giving rise to the damage).

8. Where both a Controller and a Processor (or more than one Controller or Processor), are involved in the same Processing and where they are responsible for any damage caused by Processing each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the Data Subject. Where a Controller or Processor has paid full compensation for the damage suffered, that Controller or Processor shall be entitled to claim back from the other Controllers or Processors involved in the same Processing that part of the compensation corresponding to their part of responsibility for the damage.

5.6. RESTRICTIONS ON TRANSFERS AND ONWARD TRANSFERS TO EXTERNAL PROCESSORS AND CONTROLLERS

Where a Local Data Controller decides to transfer Personal Data to a non-SERVIER entity acting whether as a Data Controller or a Data Processor, said Local Data Controller shall ensure that an adequate level of protection is provided to such Personal Data:

1. With regard to data transfers towards non-SERVIER entities **located inside the EEA or in a country recognized by the EU Commission as ensuring an adequate level of protection,** the following measures shall be implemented **:**

    a. External Processors shall be bound by a written agreement stipulating that the Processor shall act only on instructions from the Local Data Controller and shall be responsible for the implementation of the appropriate technical and organizational measures (see paragraph 5.4). Relevant Local Data Protection Officer(s) or Contact(s) in coordination with the Global Data Protection Officer, shall be able to provide templates of the appropriate clauses to a Local Data Controller within the SERVIER Organization.

b. External Controllers shall also be bound by a written agreement providing that they commit to provide appropriate security and confidentiality measures, that they will cooperate with the Local Data Controller where necessary and that they will process the transferred Personal Data in compliance with the exporter's data protection laws or at least in compliance with the data protection principles as set by the GDPR.

2. In case of Processors or Controllers not established in the EEA and in the absence of an adequacy decision by the EU Commission, a Local Data Controller may transfer Personal Data to a third country or an international organisation only if the external Controller or Processor has provided appropriate safeguards, as follows:

a. Transfers of Personal Data from the EEA to external Controllers located outside of the EEA shall comply with the European rules on cross-border data flows (Articles 46 and 49 of the GDPR), for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission 2001/497/EC or 2004/915/EC, or

b. Transfers of Personal Data from the EEA to external Processors located outside of the EEA shall comply with the rules relating to the Processors (Articles 28 and 49 of the GDPR) in addition to the rules on cross-border data flows (Articles 46 of the GDPR), for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission on February, 5, 2010 (c2010/0593), or

c. Transfers of Personal Data from the EEA to external Controllers or Processors located outside of the EEA shall be subject to the adoption by the Controller or Processor in the third country of an approved code of conduct together with binding and enforceable commitments to apply the appropriate safeguards, including as regards data subjects' rights, or

d. Transfers of Personal Data from the EEA to third countries shall be towards appropriately certified external Controllers or Processors located outside of the EEA and accompanied by binding and enforceable commitments of the external Controller or

Processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights, or

e. Transfers of Personal Data from the EEA to external Processors located outside of the EEA shall be subject to the implementation by the external Data Processor of appropriately approved Data Processor's Binding Corporate Rules along with a contract providing that the external Processor will process the transferred data in compliance with its Data Processor Binding Corporate Rules.

5.7. TRAINING PROGRAMS

Any SERVIER Employee who collects, processes or has access to Personal Data or who is involved in the development of tools used to process Personal Data shall be provided with training programs in order to improve their practical skills and knowledge that relate to data protection and data protection issues, especially the requirements under the BCRs:

1. BCRs and all related guidelines, procedures or policies shall be made available to every Employee.

2. Access to the BCRs and all related guidelines, procedures or policies shall be granted to every new Employee of SERVIER. Internal notices shall also be transmitted within the SERVIER Organization to raise awareness of the BCRs.

3. New Employees who collect, process, or have access to Personal Data shall follow data protection training. These trainings shall be organized in accordance with the data protection training program.

4. At local level, each relevant Local Data Protection Officer or Contact shall at its own discretion enhance the data protection training program described above by adding any relevant local data protection requirement. Data protection training program shall be reviewed and approved by experienced SERVIER personnel and the Global Data Protection Officer.

5.8. AUDIT PROGRAM

Data protection audits shall be carried out on a regular basis (subject to more stringent local laws, but at least one audit every 3 years) by internal or external accredited audit teams to ensure that the BCRs and all related policies, procedures or guidelines are updated and applied.

1. Data Protection audits shall cover all aspects of the BCRs and all related policies, procedures or guidelines, including methods of ensuring that corrective measures will take place (see **SERVIER Data Protection audit work program**). However, the scope of each audit can be strengthened to limited aspects of the BCRs and/or the related policies, procedures or guidelines, including methods of ensuring that corrective measures will take place.

2. Data Protection audits shall be decided directly by the Global Data Protection Officer or upon specific request of the Head Controller, a Local Data Controller or a Local Data Protection Officer or Contact. The results of all audits shall be communicated to the Head Controller's board of directors, and the Local Data Controller, the relevant Local Data Protection Officer or Contact and/or to the Global Data Protection Officer.

3. The relevant Supervisory Authorities shall have access to the results of the audit upon request. Each Local Data Controller shall accept to be audited by a Supervisory Authority if required.

   Based on the audit results and the reports mentioned in section 6.2 below, the Head Controller and/or the Global Data Protection Officer shall decide any appropriate legal, technical or organizational security measures in order to improve data protection management within the SERVIER Organization, both at global and local levels.

6. BINDINGNESS OF THE BCRs

6.1. INTERNAL BINDING NATURE

The present BCRs bind all SERVIER Companies which have signed the present BCRs or the BCRs intra-group agreement (Appendix 4) setting out and expressing their acceptance of the BCRs.

Each SERVIER Company that signs the present BCRs or the BCRs intra-group agreement is responsible for administering and overseeing the implementation of these BCRs, including making these BCRs binding upon the Employees who have a duty to comply with the obligations set out therein.

Pursuant to applicable local law, the BCRs are made binding towards the Employees either through work employment contracts or through collective agreements or through relevant company policies in which the BCRs have been incorporated.

6.2. COMPLIANCE AND SUPERVISION OF COMPLIANCE

SERVIER commits to designate a Date Protection Officer where required in line with Article 37 of the GDPR or any other person or entity (such as a chief privacy officer) with responsibility to monitor compliance with the BCRs enjoying the highest management support for the fulfilling of this task. The DPO shall directly report to the highest management level, according to Article 38-3 of the GDPR.

SERVIER also commits to establish a data protection network composed of Data Protection Officers and Contacts appointed at local levels and worldwide and a Global Data Protection Officer.

At local level, each Local Data Protection Officer or Contact shall be responsible for the implementation of the BCRs. Thus:

1. Local Data Protection Officers or Contacts shall inform and advise the Local Data Controllers and the Employees who carry out Processing of their obligations.

2. Local Data Protection Officers or Contacts shall take all reasonable steps to make sure that Local Data Controllers comply with the provisions of the BCRs (including said provisions concerning training of staff involved in Processing operation and audits). To this end, a **"BCR compliance check list"** shall be used at local levels to make compliance checks. Data Protection audits ultimately decided by the Global Data Protection Officer may focus on how these compliance checks are made at the local level (see paragraph 5.8 above).

3. Each Local Data Protection Officer or Contact in coordination with the Global Data Protection Officer, shall be at the disposal of Local Data Controllers, Processors that are members of the SERVIERSERVIER Organization and Data Subjects to provide any help with regard to a data protection issue, especially the BCRs, when necessary.

4. Each Local Data Protection Officer or Contact must provide advice where requested as regards the conduct of any data protection impact assessment and monitor its performance where required (see **Data Protection Impact Assessment methodology**).

5. Each Local Data Protection Officer or Contact, in coordination with the Global Data Protection Officer, shall report every year to the Head Controller about all the actions and measures taken with regard to data protection issues (data protection training program, Records of Processing Activities, management of complaints, etc.), especially the implementation of the BCRs.

6. Each Local Data Protection Officer or Contact shall regularly report to the Global Data Protection Officer about the complaints settled at local levels, with a view to taking corrective actions and improving guidelines and procedures implemented within the SERVIER Organization, where the complaints may have revealed a "gap" in terms of data protection.

7. Each Local Data Protection Officer or Contact, in coordination with the Global Data Protection Officer, shall provide, when appropriate, any appropriate templates (i.e. notices of information,

clauses, etc.) to each Local Data Controller within the SERVIER Organization for any purpose related to a data protection issue.

8. Each Local Data Protection Officer or Contact shall cooperate with the Supervisory Authorities and act as the contact point for the Supervisory Authorities on issues relating to Processing.

Furthermore, in terms of supervision of compliance, specific measures shall be taken to ensure the right implementation of the BCRs:

1. The Global Data Protection Officer shall regularly report to the Head Controller about the implementation of the BCRs within each Local Data Controller and within each Processor that is a member of the SERVIER Organization.

2. The results of all reports made by the Global Data Protection Officer shall be communicated to the Head Controller (especially to the Head Controller's management), and the Local Data Controller, and/or the relevant Local Data Protection Officer or Contact.

3. Based on the audit results (see paragraph 5.8 above) and the reports mentioned above, the Head Controller (especially the Head Controller's executive board), the Global Data Protection Officer, the relevant Local Data Controller(s), and the Local Data Protection Officer(s) or Contact(s) shall decide on any appropriate measure in order to improve data protection management within the SERVIER Organization, both at global and/or local levels. Any measure that would be decided by one of the relevant stakeholders shall be taken in cooperation with the others who shall be duly informed about such decision, when appropriate.

4. The Global Data Protection Officer will liaise with the Lead Supervisory Authority which is also acting as lead supervisory authority under the meaning of Article 56 of the GDPR.

6.3. THIRD PARTY BENEFICIARY RIGHTS

1. A Data Subject who claims to have suffered damage as a direct result of a violation of the provisions of the BCRs listed below and/or Appendix 1 of these BCRs, and who either is not satisfied with the resolution of their complaint, as described in paragraph 5.4, or desires to bypass the internal complaint mechanism and bring their complaint directly to the competent Supervisory Authority, may seek to enforce their third party beneficiary rights before the competent Supervisory Authority or before the competent court of the EU Member States according to the principles and terms as set out below. The **BCRs complaint procedure** shall support Data Subjects' ability to address any data protection complaint internally. Data Subjects are however free to lodge a complaint directly with the competent Supervisory Authority or the competent court of the EU Member States as provided by local Applicable Data Protection Laws.

2. A Data Subject shall have the right to enforce, as a third party beneficiary, the provisions of the BCRs related to:
    - Purpose limitation (see paragraph 2.2 and Appendix 1)
    - Data quality and data minimization (see paragraph 2.2 and Appendix 1)
    - Lawfulness principles for Processing Personal Data and Special Categories of Data (see paragraph 2.2 and Appendix 1)
    - Fairness and Transparency principles and right to information and easy access to the BCRs (see paragraph 5.1)
    - Rights of access, rectification, erasure, restriction of Processing, objection to Processing and right to data portability (see paragraph 5.2)
    - Rights in case automated individual decisions-making (including Profiling) are taken (see paragraph 5.3. and Appendix 1)
    - Security and confidentiality (see paragraph 5.5)
    - Restrictions on onward transfers outside of the SERVIER Organization of companies (see paragraph 5.6)
    - National legislation preventing respect of BCRs (see paragraph 7.2)
    - Right to complain through the internal complaint mechanism (see paragraph 5.4)
    - Cooperation duties with Supervisory Authorities (see paragraph 6.6)
    - Liability and jurisdiction provisions (see paragraphs 6.3 and 6.4)

As a rule regarding jurisdiction for any claim, each Data Subject shall have the right to lodge a complaint, at its best convenience:

- with the competent supervisory authority. It is up to the Data Subject to choose between the supervisory authority in the Member State of his habitual residence, place of work or place of the alleged infringement.
- or before the competent court. It will be the choice for the Data Subject to act before the courts where the Local Data Controller or Processor has an establishment or where the
- Data Subject has his or her habitual residence.

3. According to the relevant provisions in paragraph 6.3.1, each Data Subject who has suffered damage shall be entitled to obtain redress and, where appropriate, receive compensation in case of any breach of one of the enforceable elements as enumerated above as may be ordered by the appropriate court or competent Supervisory Authority or as decided according to the internal complaint mechanism, if used.

4. The BCRs shall always be readily available to every Data Subject, in the conditions described in paragraph 5.1.

5. SERVIER Companies bound by the BCRs shall abide by a decision of a competent court or a competent regulatory authority (provided such court or authority is based in the EEA country in which the Data Exporter is established) which is final and against which no further appeal is possible.

6.4. LIABILITY

Every SERVIER Company who is a BCR member exporting data out of the EEA on the basis of the BCR will be liable for any breaches of the BCRs by the SERVIER Company or BCR member established outside the EEA which received the data from this SERVIER Company, BCR member located in the EEA.

The SERVIER Company that has accepted liability will also have the burden of proof to demonstrate that the SERVIER Company outside the EEA is not liable for any violation of the rules which has resulted in the data subject claiming damages.

If the SERVIER Company that has accepted liability can prove that the SERVIER Company outside the EEA is not responsible for the event giving rise to the damage, it may discharge itself from any responsibility.

6.5. SANCTIONS

Would a violation of the BCRs, either by Local Data Controller representatives or Employees, be identified, any appropriate disciplinary sanction or judicial action may be imposed, in accordance with local law, on the initiative of the Head Controller, the Head Data Protection Officer, the Local Data Controller, the relevant Local Data Protection Officer or Contact.

Thus, the Head Data Protection Officer and each Local Data Controller and Local Data Protection Officer or Contact shall pay specific attention to any audit results (see paragraph 5.8) establishing non-compliance issues against representatives or Employees, especially in case of non-compliance with the Data Protection Principles and the applicable guidelines, procedures and policies related to the implementation of the BCRs.

6.6. MUTUAL ASSISTANCE AND COOPERATION WITH SUPERVISORY AUTHORITIES

SERVIER Companies bound by the BCRs commit to a full cooperation with the Supervisory Authorities who have competent jurisdiction, particularly by responding within a reasonable time frame to their requests concerning the interpretation and application of the BCRs and to comply with their advice and recommendations in this respect, provided they are consistent with applicable law.

SERVIER Companies bound by the BCRs commit to accept audits from the competent Supervisory Authorities as well as provide the results of the audits upon request.

Furthermore, members of SERVIER Companies bound by the BCRs shall cooperate and assist each other to handle a request or complaint from an individual (see paragraph 5.3) or inquiry by Supervisory Authorities.

Each competent Supervisory Authority has the power to supervise the implementation of the BCRs.

7. FINAL PROVISIONS

7.1. RELATIONSHIPS BETWEEN NATIONAL LAWS AND THE BCRs

SERVIER undertakes that the SERVIER Companies and Employees of the SERVIER Organization shall comply with the provisions of the BCRs, as well as with the provisions of the GDPR and 2002/58/EC Directive and local Applicable Data Protection Laws.

Where the local Applicable Data Protection Laws require a higher level of protection for Personal Data, it always will take precedence over the BCRs.

7.2. ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF BCRs

If a Local Data Controller has reason to believe that legislation applicable to the Local Data Controller prevents the Local Data Controller from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by the BCRs, the Local Data Controller will promptly inform the Head Data Protection Officer (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

Where there shall be conflict between local Applicable Data Protection Law and the commitments in the BCRs, the relevant Local Data Protection Officer or Contact shall inform the Head Data Protection Officer. The Head Data Protection Officer shall take a responsible decision on which appropriate actions to be undertaken.

In case of doubt and where a major conflict exists between local Data Protection Law and the BCRs, the Head Data Protection Officer shall consult the competent Data Protection Authorities, in case of doubt, and is responsible for making a decision regarding the conflict.

More particularly, where any legal requirement a Local Data Controller is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by the BCRs, the problem should be reported to the competent Data Protection Authorities. This includes any legally binding request for disclosure of the personal data by a law enforcement authority or state security body. In such a case, the competent Data Protection Authorities should be clearly informed about the request, including information about the Personal Data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

If in specific cases the suspension and/or notification are prohibited, the requested Local Data Controllers will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

If, in the above cases, despite having used its best efforts, the requested Local Data Controller is not in a position to notify the competent Data Protection Authorities, this Controller commits to annually providing general information on the requests it received to the competent Data Protection Authorities (e.g. number of applications for disclosure, type of Personal Data requested, requester if possible, etc.).

In any case, Transfers of Personal Data by a Local Data Controller to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

7.3. UPDATES OF THE BCRs

In case of changes in laws, in SERVIER procedures or in the scope of the BCRs, the terms of the BCRs may be updated on the initiative of the Head Controller, in coordination with the Head Data Protection Officer**.**

Any update of the BCRs shall be recorded and kept by the Head Data Protection Officer. The Head Data Protection Officer keeps an updated list of the members of the SERVIER Organization. These changes shall also be communicated to SERVIER Companies which have signed the present BCRs or the intra-group agreement (Appendix 4).

No transfer based on the BCRs shall be made to a new SERVIER Company until this new Company is effectively bound by the BCRs and can deliver compliance to the same.

SERVIER undertakes that any update of the BCRs will be provided to the competent Supervisory Authorities through the Lead Supervisory Authority. Having said that:

- any changes which would affect the level of protection offered by the BCRs or will significantly affect the BCRs will be provided to the Leading Supervisory Authority promptly, which will consider whether this affects the approval previously issued for the BCR;
- Other modifications will be provided to the Lead Data Protection Authority once a year.

In addition, SERVIER undertakes to provide the necessary information about any updates to the rules to the Data Subjects upon request.

7.4. ENTRY INTO EFFECT AND TERMINATION

The BCRs shall take effect on the date when the respective entity of SERVIER signs Appendix4 of this BCRs agreement and, as a consequence, is legally bound.

Each entity of SERVIER recognizes to be bound by the BCRs, from the date of signature of the Appendix 4 of the BCRs agreement and without any other formalities, with respect to other SERVIER entities already bound or about to be bound from the date of their signature, notwithstanding the date and place of signature of a BCRs agreement by each other entity of SERVIER involved, and provided that the terms of the BCRs are strictly identical between each other. Except if an entity of SERVIER is able to prove that its signed BCRs agreement is not strictly identical to the ones signed by other entities, it expressly and irrevocably disclaims challenging the evidence that it is bound by the terms of the BCRs.

In the event that a Local Data Exporter or a Local Data Importer would be found in substantial or persistent breach of the terms of the BCRs, the Head Controller may temporarily suspend the transfer of

Personal Data until the breach is remedied. Should the breach not be remedied in due time, the Head Controller shall take the initiative to terminate the BCRs intra-group agreement with respect to that specific Local Data Exporter or Local Data Importer. In such a case, the Local Data Exporter or Local Data Importer shall take every necessary step in order to comply with the European rules on cross-border data flows (Article 46 of the GDPR), for instance by using the EU Standard Contractual Clauses approved by the EU Commission.

7.5. APPLICABLE LAW / JURISDICTION

The provisions of the BCRs shall be governed by the Applicable Data Protection Law.

In accordance with paragraph 6.4, jurisdiction shall be attributed to the courts of the Local Data Importer or Local Data Exporter.

7.6. INTERPRETATION OF TERMS

In case of discrepancies between the BCRs and the Appendices, the main body of the BCRs shall prevail. In case of discrepancies between the BCRs including its Appendices and other global or local SERVIER policies, SERVIER procedures or SERVIER guidelines, the BCRs shall prevail. In case of discrepancies or inconsistency, the terms of the BCRs shall always be interpreted and governed by the provisions of the GDPR and E-Privacy Directive.

To be signed by each Company of SERVIER bound by the present BCRs

*

* *

IN WITNESS WHEREOF, the following Companies of SERVIER undertake to comply with the provisions of the BCRs of SERVIER AS OF THE DATE OF SIGNATURE STATED BELOW.

This undertaking will be relevant for:

- the version dated [to be completed]
- and for any updated BCRs that would be notified according to paragraphs 7.3 and 7.4 of the BCRs

On: _____ (Date of signature)

► **TO BE COMPLETED**

Name:
Title:

APPENDICES

- **APPENDIX 1 – DATA PROTECTION PRINCIPLES**
- **APPENDIX 2 – LIST OF SERVIER COMPANIES BOUND BY THE BCRS**
- **APPENDIX 3 – NATURE AND PURPOSES OF THE PERSONAL DATA BEING TRANSFERRED WITHIN THE SCOPE OF THE BCRS**
- **APPENDIX 4 – BCRS INTRA-GROUP AGREEMENT**

APPENDIX 1: DATA PROTECTION PRINCIPLES

Within the scope of the BCRs, any transfer of Personal Data to a third country which does not ensure an adequate level of protection shall always comply with the following data protection principles, set out by the GDPR.

FAIRNESS & TRANSPARENCY

Fairness requires that the data subject be informed of the existence of the Processing operation and its purposes.

Any information and communication relating to the processing of the Data Subjects' Personal Data shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. That principle concerns, in particular, information to the Data Subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of Personal Data concerning them which are being processed.

The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the Data Subject, the information may be provided orally, provided that the identity of the Data Subject is proven by other means.

PURPOSE LIMITATION

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

Further processing may be however allowed if the relevant consent of the Data Subject concerned is obtained or where authorized by a Union or Member State law. In all the other cases and according to Article 6.4. of the GDPR, the Controller shall ascertain whether the processing for another purpose is

compatible with the purpose for which the Personal Data are initially collected. To do so, the Controller shall take into account, inter alia:

a. any link between the purposes for which the Personal Data have been collected and the purposes of the intended further processing;
b. the context in which the Personal Data have been collected, in particular regarding the relationship between data subjects and the controller;
c. the nature of the Personal Data, in particular whether special categories of Personal Data are processed, or whether Personal Data related to criminal convictions and offences are processed;
d. the possible consequences of the intended further processing for data subjects;
e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Further Processing of data for archiving purposes in the public interest scientific or historical research purposes or statistical purposes shall not be considered as incompatible provided implementation of appropriate safeguards for the rights and freedom of the Data Subjects.
Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimization.

DATA MINIMIZATION, LIMITED STORAGE PERIODS AND DATA QUALITY

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and/or processed (data minimization).
Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are processed. Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the Data Subject (limited storage periods).

Personal Data shall be accurate and, where necessary, kept up to date (accuracy).

DATA PROTECTION BY DESIGN AND BY DEFAULT:

Data protection by design: the Local Data Controller must implement, both at the time of the determination of the means for Processing and at the time of the Processing itself, appropriate technical and organizational measures (such as Pseudonymization), which are designed to implement data-protection principles (such as data minimization), in an effective manner and to integrate the necessary safeguards into the Processing.

Data protection by default: the Local Data Controller must 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.

LAWFULNESS OF PROCESSING OF PERSONAL DATA

Personal Data shall be processed only if:

- the Data Subject has given its Consent to the Processing of his or her Personal Data for one or more specific purposes;
- Processing 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;
- Processing is necessary for compliance with a legal obligation to which the Local Data Controller is subject;
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Local Data Controller;
- Processing is necessary for the purposes of the legitimate interests pursued by the Local Data Controller or by the Third Party except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

LAWFULNESS OF PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

Special Categories of Personal Data, especially Personal Data Concerning Health, shall be processed only if:

- the Data Subject has given its explicit Consent to the Processing of those Special Categories of Personal Data, for one or more specified purposes, except where the applicable laws prohibit it;
- the Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller and the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by Union or national law or a collective agreement providing for adequate safeguards for the fundamental rights and the interests of the Data Subjects;
- the Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving its Consent;
- the Processing is carried out in the course of its legitimate activities with appropriate safeguards 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 or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data is not disclosed outside the body without the Consent of the Data Subjects;
- the Processing relates to Special Categories of Personal Data which is manifestly made public by the Data Subject;
- the Processing of Special Categories of Personal Data is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- the Processing of the Special Categories of 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 national law or pursuant to contract with a health professional and subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Other specific categories of data may be subject to local data protection requirements provided by each national law. In particular, Processing of data relating to criminal convictions and offences or related security measures may be carried out only under the control of official authority, or when the Processing is authorized by national law providing for appropriate safeguards for the rights and freedoms of Data Subjects. In addition, national law may further determine the specific conditions for

the Processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the Data Subject pursuant to the national law.

SECURITY OF PERSONAL DATA

Appropriate technical and organizational measures shall be implemented to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of or access to and against all other unlawful forms of Processing (see paragraph 5.5).

ONWARD TRANSFERS TO ORGANIZATIONS NOT BOUND BY BCRS

When Personal Data is intended to be transferred to a non-SERVIER Company, adequate safeguards have to be implemented (se paragraph 5.6).

ACCOUNTABILITY

The Local Data Controller shall be responsible for, and be able to demonstrate compliance with the present data protection principles (**accountability**).

In order to demonstrate compliance, BCR members need to maintain a record of all categories of processing activities carried out in line with the requirements as set out in Article 30.1 of the GDPR.

In order to enhance compliance and when required, data protection impact assessments should be carried out for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons (GDPR Article 35). Where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the Local Data Controller to mitigate the risk, the competent Supervisory Authority, prior to the processing, should be consulted (GDPR Article 36).

APPENDIX 2: LIST OF SERVIER COMPANIES BOUND BY THE BCRs

Each Company will be bound by the BCRs after signing the present BCRs or after signing the BCRs intra-group agreement in appendix 4.

HEAD CONTROLLER	**SERVIER SAS**
Registered address	50 rue Carnot, 92284 SURESNES
Legal representative	Olivier LAUREAU
Global Data Protection Officer	Natacha UDO-BEAUVISAGE

1. SERVIER Companies located in the EEA

Country	AUSTRIA
LOCAL DATA CONTROLLER	Servier Austria GmbH
Registered address	Mariahilferstrasse 20, 1070 Wien

Country	BELGIUM
LOCAL DATA CONTROLLER	Servier Benelux
Registered address	57, bvd International - Riversade Business Park - 1070 Bruxelles

Country	BELGIUM
LOCAL DATA CONTROLLER	Eutherapie Benelux
Registered address	57, bvd International - Riversade Business Park - 1070 Bruxelles

Country	BELGIUM
LOCAL DATA CONTROLLER	Servier R&D Benelux
Registered address	57, bvd International - Riversade Business Park - 1070 Bruxelles

Country	BELGIUM
LOCAL DATA CONTROLLER	Daxispharma
Registered address	57, bvd International - Riversade Business Park - 1070 Bruxelles

Country	BELGIUM
LOCAL DATA CONTROLLER	Bureau de représentation Les Laboratoires Servier

Registered address	41, avenue des Arts - 1040 Bruxelles

Country	BULGARIA
LOCAL DATA CONTROLLER	Servier Bulgaria EOOD
Registered address	14 boul. Tzar Osvoboditel, municipalité Sredetz, Sofia

Country	BULGARIA
LOCAL DATA CONTROLLER	Servier Medical EOOD
Registered address	14 boul. Tzar Osvoboditel, municipalité Sredetz, Sofia

Country	CROATIA
LOCAL DATA CONTROLLER	Servier Pharma d.o.o.
Registered address	Tuškanova 37, 10000 Zagreb

Country	CZECH REPUBLIC
LOCAL DATA CONTROLLER	Servier s.r.o.
Registered address	Na Florenci 2116/15, Prague 1, code postal 110 00

Country	DENMARK
LOCAL DATA CONTROLLER	Servier Danmark A/S
Registered address	Lyngbyvej 2 - DK-2100 Copenhague

Country	ESTONIA
LOCAL DATA CONTROLLER	Servier Laboratories OÜ
Registered address	

Country	FRANCE
LOCAL DATA CONTROLLER	Servier S.A.S
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Institut de Recherches Servier
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Les Laboratoires Servier
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Servier Healthcare
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Servier Outre-Mer
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Servier Monde
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Actam
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Adir
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Institut de Recherches Internationales Servier
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Servier International
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Amplex
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Iris et Compagnie - Développement
Registered address	50, rue Carnot - 92284 Suresnes cedex

Country	FRANCE

LOCAL DATA CONTROLLER	Arts et Techniques du Progrès Technologie Servier
Registered address	25, rue Eugène Vignat - 45000 Orléans

Country	FRANCE
LOCAL DATA CONTROLLER	Biogaran
Registered address	15, bvd Charles de Gaulle - 92700 Colombes

Country	FRANCE
LOCAL DATA CONTROLLER	Les Laboratoires Servier Industrie
Registered address	905, route de Saran - 45520 Gidy

Country	FRANCE
LOCAL DATA CONTROLLER	Biologie Servier
Registered address	905, route de Saran - 45520 Gidy

Country	FRANCE
LOCAL DATA CONTROLLER	Oril Industrie
Registered address	13, rue Auguste Desgenetais - 76210 Bolbec

Country	FRANCE
LOCAL DATA CONTROLLER	Servier France
Registered address	35, rue de Verdun - 92284 Suresnes cedex

Country	FRANCE
LOCAL DATA CONTROLLER	Servier Affaires Médicales
Registered address	35, rue de Verdun - 92284 Suresnes cedex

Country	FINLAND
LOCAL DATA CONTROLLER	Servier Finland Oy
Registered address	Äyritie 22A, Plaza Business Park Tuike, 01510 Vantaa

Country	GERMANY
LOCAL DATA CONTROLLER	Servier Deutschland GmbH
Registered address	Elsenheimerstrasse 53, 80687 Munchen

Country	GERMANY

LOCAL DATA CONTROLLER	Servier Forschung und Pharma-Entwicklung GmbH
Registered address	Elsenheimerstrasse 53, 80687 Munchen

Country	GREECE
LOCAL DATA CONTROLLER	Servier Hellas Pharmaceutique E.P.E.
Registered address	7 Fragkoklissias Street, 15125 Marousi (Athènes)

Country	HUNGARY
LOCAL DATA CONTROLLER	Servier Hungaria Kft
Registered address	Vaci út 1-3, Westend Office, Tour B, 3ème étage 1062 Budapest

Country	HUNGARY
LOCAL DATA CONTROLLER	Institut de Recherche Servier de Chimie Médicinale Société Anonyme Fermée
Registered address	"Zahony utca 7, 1031 Budapest"

Country	HUNGARY
LOCAL DATA CONTROLLER	Egis Pharmaceuticals Private Limited Company
Registered address	Keresztúri út 30-38, 1106 Budapest

Country	IRELAND
LOCAL DATA CONTROLLER	Servier (Ireland) Industries Limited
Registered address	Gorey Road, County Wicklow, Arklow

Country	IRELAND
LOCAL DATA CONTROLLER	Supram Limited
Registered address	Gorey Road, County Wicklow, Arklow

Country	IRELAND
LOCAL DATA CONTROLLER	Servier Laboratories (Ireland) Limited
Registered address	1/F, Block 2, West Pier Business Campus, Dun laoghaire, Dublin 4, Dublin

Country	IRELAND
LOCAL DATA CONTROLLER	Irsur DAC
Registered address	3rd Floor,The Metropolitan Building,James Joyce Street, Dublin 1,Dublin

Country	ITALY
LOCAL DATA CONTROLLE	Servier Italia S.P.A.
Registered address	85, Via Luca Passi, 00100 Rome

Country	ITALY
LOCAL DATA CONTROLLE	Istituto Farmaco Biologico Stroder S.R.L.
Registered address	85, Via Luca Passi, 00100 Rome

Country	ITALY
LOCAL DATA CONTROLLE	Istituto di Ricerca Servier S.R.L.
Registered address	85, Via Luca Passi, 00100 Rome

Country	LATVIA
LOCAL DATA CONTROLLE	SIA Servier Latvia
Registered address	11/F, Duntes street 11, 1013 Riga

Country	LITHUANIA
LOCAL DATA CONTROLLE	UAB Servier Pharma
Registered address	8/F, Verslo centras, Konstitucijos pr. 7, 09308 Vilnius

Country	LUXEMBOURG
LOCAL DATA CONTROLLER	Servier Luxembourg S.A
Registered address	3A, rue Guillaume Kroll, L-1882 Luxembourg

Country	NETHERLANDS
LOCAL DATA CONTROLLER	Servier International B.V
Registered address	Promenadeplein 125, 2711 AB Zoetermeer

Country	NETHERLANDS
LOCAL DATA CONTROLLER	Servier Nederland B.V
Registered address	Promenadeplein 125, 2711 AB Zoetermeer

Country	NETHERLANDS
LOCAL DATA CONTROLLER	Nederiane B.V
Registered address	Promenadeplein 125, 2711 AB Zoetermeer

Country	NETHERLANDS
LOCAL DATA CONTROLLER	Nereax B.V
Registered address	Promenadeplein 125, 2711 AB Zoetermeer

Country	NETHERLANDS
LOCAL DATA CONTROLLER	Ixor N.V
Registered address	Promenadeplein 125, 2711 AB Zoetermeer

Country	NETHERLANDS
LOCAL DATA CONTROLLER	Serpharm B.V
Registered address	Promenadeplein 125, 2711 AB Zoetermeer

Country	NETHERLANDS
LOCAL DATA CONTROLLER	Servier Nederland Farma B.V
Registered address	Kanaalpark 140, 2321 JV Leiden

Country	NETHERLANDS
LOCAL DATA CONTROLLER	Arcova Investment B.V
Registered address	Promenadeplein 125, 2711 AB Zoetermeer

Country	POLAND
LOCAL DATA CONTROLLER	Servier Polska Sp. Z o.o.
Registered address	"Ul. Jana Kazimierza 10, 01-248 Varsovie"

Country	POLAND
LOCAL DATA CONTROLLER	Servier Polska Services Sp. Z o.o.
Registered address	"Ul. Jana Kazimierza 10, 01-248 Varsovie"

Country	POLAND
LOCAL DATA CONTROLLER	"Anpharm" Przedsiebiorstwo Farmaceutyczne Spolka Akcyjna
Registered address	"Ul. Annopol 6 B, 03-236 Varsovie"

Country	PORTUGAL
LOCAL DATA CONTROLLER	Armedic Especialidades Farmaceuticas Lda.
Registered address	128 Av. Antonio Augusto de Aguiar, 1069-133, Lisbonne

Country	PORTUGAL
LOCAL DATA CONTROLLER	Lusoterapia Sociedade Comercial de Producao Quimico-Farmaceutica Lda.
Registered address	128 Av. Antonio Augusto de Aguiar, 1069-133, Lisbonne

Country	PORTUGAL
LOCAL DATA CONTROLLER	Servier Portugal Especialidades Farmaceuticas Lda.
Registered address	128 Av. Antonio Augusto de Aguiar, 1069-133, Lisbonne

Country	PORTUGAL
LOCAL DATA CONTROLLER	Socofar Sociedade Comercial de Especialidades Farmaceuticas Lda.
Registered address	128 Av. Antonio Augusto de Aguiar, 1069-133, Lisbonne

Country	ROMANIA
LOCAL DATA CONTROLLER	Sermedic S.R.L
Registered address	S-Park, str. Tipografilor nr 11-15, Corp A2.2, etaj 3, Sector 1, 013714 Bucarest

Country	ROMANIA
LOCAL DATA CONTROLLER	Servier Pharma S.R.L
Registered address	S-Park, str. Tipografilor nr 11-15, Corp A1, etaj 3, Sector 1, 013714 Bucarest

Country	SLOVAKIA
LOCAL DATA CONTROLLER	Servier Slovensko spol s r.o.
Registered address	Pribinova 10, 81109 Bratislava

Country	SLOVENIA
LOCAL DATA CONTROLLER	Servier Pharma d.o.o.
Registered address	1000 Ljubljana, Podmilščakova 24

Country	SPAIN
LOCAL DATA CONTROLLER	Danval, S.A.

Registered address	Avenida de los Madroños 33, Parque del Conde de Orgaz, 28043 Madrid

Country	SPAIN
LOCAL DATA CONTROLLER	Laboratorios Lestral, S.A.
Registered address	Avenida de los Madroños 33, Parque del Conde de Orgaz, 28043 Madrid

Country	SPAIN
LOCAL DATA CONTROLLER	Laboratorios Servier, S.L.
Registered address	Avenida de los Madroños 33, Parque del Conde de Orgaz, 28043 Madrid

Country	SWEDEN
LOCAL DATA CONTROLLER	Servier Sverige AB
Registered address	Frösundaviks Allé 1, Haga 2:8, 16970 Solna

Country	UNITED KINGDOM
LOCAL DATA CONTROLLER	Servier Laboratories Limited
Registered address	Sefton House - Sefton Park - Bells Hill, Stoke Poges - SL2 4JS Slough

Country	UNITED KINGDOM
LOCAL DATA CONTROLLER	Servier Research & Development Limited
Registered address	Sefton House - Sefton Park - Bells Hill, Stoke Poges - SL2 4JS Slough

2. Local SERVIER Companies located outside the EEA

Country	ALGERIA
LOCAL DATA CONTROLLER	Biogaran Algerie
Registered address	33, rue des Pins Hydra - 16035 Alger

Country	ARMENIA
LOCAL DATA CONTROLLER	LLS Representative Office
Registered address	

Country	ARGENTINA
LOCAL DATA CONTROLLER	Servier Argentina S.A.
Registered address	Avenida Libertador 5926/54, Piso 8,1428 Buenos Aires

Country	AUSTRALIA
LOCAL DATA CONTROLLER	Servier Laboratories (Aust,) PTY, LTD.
Registered address	8 Cato street, 3122 Hawthorn Victoria

Country	AZERBAIDZAN
LOCAL DATA CONTROLLER	Servier Azerbaïdjan LLC
Registered address	1033 settlement, Tbilisi avenue 35, Baku, AZ1065, Azerbaijan

Country	BELARUS
LOCAL DATA CONTROLLER	LLS Representative Office
Registered address	

Country	BRAZIL
LOCAL DATA CONTROLLER	Laboratórios Servier Do Brasil LTDA.
Registered Address	Estrada dos Bandeirantes, 4211,Curicica, Jacarepaguá, 22775-113, Rio de Janeiro

Country	BRAZIL
LOCAL DATA CONTROLLER	Pharlab Indústria Farmacêutica Ltda.
Registered Address	Rua Sao Francisco, n° 1300, Bairro Americo Silva, CEP 35590 - 000, Lagoa de Prata, Mina Gerais, Brasil

Country	CAMBODIA
LOCAL DATA CONTROLLER	SI Representative Office
Registered address	

Country	CANADA
LOCAL DATA CONTROLLER	**Servier Canada Inc**
Registered address	235 bvd Armand Frappier - H7V 4A7 LAVAL - Canada

Country	CHINA
LOCAL DATA CONTROLLER	**Servier (Beijing) Pharmaceutical research & Development Co., LTD**
Registered address	Unit 11-14, Unit 15A, 6th floor, west buidling, World Financial Centre, N°1 Dongsanhuan road (middle), Chaoyang district, 100020 Beijing, P.R. China

Country	CHINA
LOCAL DATA CONTROLLER	**Servier (Tianjin) Pharmaceutical Company Limited**
Registered address	10th Avenue, TEDA, Tianjin, China

Country	COLOMBIA
LOCAL DATA CONTROLLER	Laboratorios Servier de Colombia S.A.S.
Registered address	Edificio 98-28,Transversal 19A# 98-28, Bogotá, D.C.

Country	ECUADOR
LOCAL DATA CONTROLLER	**LLS Representative Office**
Registered address	

Country	EGYPT
LOCAL DATA CONTROLLER	**Servier Egypt Industries Limited**
Registered address	1st Industrial Zone, Plot n°37, 6 of October City - Giza Governate - Egypt

Country	EGYPT
LOCAL DATA CONTROLLER	**LLS Scientific bureau**
Registered address	

Country	GEORGIA
LOCAL DATA CONTROLLER	**LLS Representative Office**
Registered address	

Country	HONG KONG
LOCAL DATA CONTROLLER	**Servier Hong Kong Limited**
Registered address	42/F, 248 Queen's road east, Wanchai, Hong-Kong

Country	INDIA
LOCAL DATA CONTROLLER	**Serdia Pharmaceuticals (India) Pvt. Ltd.**
Registered address	Serdia House, Off. Dr. S.S. Rao Road, 400 012 Parel, Mumbai, India

Country	INDONESIA
LOCAL DATA CONTROLLER	**P.T. Servier Indonesia**
Registered address	Menara kadin Indonesia, 18/F, JL. HR. Rasuna Said Blok, X-5, Kav 2-3, 12950 Jakarta

Country	IVORY COAST
LOCAL DATA CONTROLLER	**LLS Representative Office**
Registered address	

Country	JAPAN
LOCAL DATA CONTROLLER	**Nihon Servier Kabushiki Kaisha**
Registered address	Hongo MK Building, 28-34 Hongo 1-chome, Bunkyo-ku, 113-0033-Tokyo

Country	KAZAKSHSTAN
LOCAL DATA CONTROLLER	**Servier Kazakhstan LLP**
Registered address	310 G, Dostyk avenue, Almaty, 050020, Kazakhstan

Country	KAZAKSHSTAN
LOCAL DATA CONTROLLER	**LLS Representative Office**
Registered address	

Country	KOREA
LOCAL DATA CONTROLLER	**Servier Korea LTD.**
Registered address	Banpo-do, Hong-ik University, Kangnam-kwan, 5th floor, 215 Seochojungang-gu, Seocho-gu, 137-802 Seoul

Country	LEBANON
LOCAL DATA CONTROLLER	**LLS Representative Office**
Registered address	

Country	MALAYSIA
LOCAL DATA CONTROLLER	**Servier Malaysia SDN. BHD.**
Registered address	Adresse opérationnelle : 1301, Level 13, Uptown 2, 2 Jalan SS 21/37, Damansara Uptown, 47400 Petaling Jaya, Selangor, Malaysia

Country	MEXICO
LOCAL DATA CONTROLLER	**Beckman Laboratories de Mexico, S.A. de C.V.**
Registered address	Dr. Barragán N° 531, Col. Narvarte, 03020 México DF

Country	MEXICO
LOCAL DATA CONTROLLER	**Laboratorios Servier (Mexico), S.A. de C.V.**
Registered address	Av. Paseo de las Palmas 525, Colonia Lomas de Chapultepec, Delegacion Miguel Hidalgo – Distrito Federal - 11 000 MEXICO

Country	MEXICO
LOCAL DATA CONTROLLER	**Nifax, S.A. de C.V.**
Registered address	Kelvin n° 27 Piso 3, Colonia Anzures, 11590 México DF

Country	MOROCCO
LOCAL DATA CONTROLLER	**Servier Maroc**
Registered address	Immeuble Zevaco, Lotissement Fath 4, Boulevard Abdelhadi Boutaleb, Casablanca, Maroc

Country	NIGERIA
LOCAL DATA CONTROLLER	**Swiss Pharma Nigeria Ltd**
Registered address	5 Dopemu Road, Agege, Lagos, Federal Republic of Nigeria

Country	NIGERIA

LOCAL DATA CONTROLLER	**Servier Pharmaceuticals Development**
Registered address	9th floor, St Nicholas House, Catholic Mission Street, Lagos Island, Federal Republic of Nigeria

Country	PAKISTAN
LOCAL DATA CONTROLLER	**Servier Research & Pharmaceuticals (Pakistan) Pvt. Ltd.**
Registered address	65 Main Boulevard, Gulberg, Lahore, Pakistan

Country	PANAMA
LOCAL DATA CONTROLLER	**Servier Centro America y Caribe, S.A.**
Registered address	Edificio P.H. Torre Panamá, Piso 25, Boulevard Costa del Este, Costa del Este, Panamá, Republic of Panamá

Country	PANAMA
LOCAL DATA CONTROLLER	**Servier Centro America Region, S.A.**
Registered address	Edificio P.H. Torre Panamá, Piso 25, Boulevard Costa del Este, Costa del Este , Panamá, República de Panamá

Country	PERU
LOCAL DATA CONTROLLER	**Laboratorios Servier Peru S.A.C.**
Registered address	Av. Alfredo Benavides 1944, Of. 502, Miraflores - LIMA 18

Country	PHILIPINNES
LOCAL DATA CONTROLLER	**Servier Philippines, INC.**
Registered address	Orion corner mercredes street 2, Bel Air Village, 1209 Makaty city

Country	RUSSIA
LOCAL DATA CONTROLLER	LLC "SERVIER RUS"
Registered address	Lesnaya Street 7, Moscow 125047, Russian Federation

Country	RUSSIA
LOCAL DATA CONTROLLER	JSC "Servier"
Registered address	Building 1/1, Sofyino village, Krasnopakhorskoe district, Moscow

	108828, Russian Federation

Country	RUSSIA
LOCAL DATA CONTROLLER	LLS Representative Office
Registered address	

COUNTRY	SAUDI ARABIA
LOCAL DATA CONTROLLER	**LLS Representative Office**
Registered address	

Country	SERBIA
LOCAL DATA CONTROLLER	**Servier D.O.O.**
Registered address	Bulevar Mihaila Pupina 10L, Novi Beograd, Srbija

COUNTRY	SERBIA
LOCAL DATA CONTROLLER	**LLS Representative Office**
Registered address	

Country	SINGAPORE
LOCAL DATA CONTROLLER	**Servier PTE LTD**
Registered address	Adresse opérationnelle : 67 Ubi Avenue 1, # 06-08 Starhub Green, Singapore 408942

Country	SRI LANKA
LOCAL DATA CONTROLLER	**SI Representative Office**
Registered address	

Country	SOUTH AFRICA
LOCAL DATA CONTROLLER	**Biogaran South Africa (PTY) Limited**
Registered address	N°4 Country Club Estate, woodlands Drive, Woodmead 2191, Gauteng, South Africa

Country	SOUTH AFRICA

LOCAL DATA CONTROLLER	**Servier Laboratories (South Africa) (Propietary) Limited**
Registered address	N°4 Country Club Estate, woodlands Drive, Woodmead 2191, Gauteng, South Africa

Country	SWITZERLAND
LOCAL DATA CONTROLLER	Servier (Suisse) S.A.
Registered address	10, rue de la Bergère Z.I. Zimeysa - 1242 Satigny (Suisse)

Country	THAILAND
LOCAL DATA CONTROLLER	**Servier (Thailand) Ltd**
Registered address	Ploenchit Center Building 15th Floor, 2 Sukhumvit Road, Kwaeng Klongtoey - Khet Klongtoey, 10110 Bangkok, Thailand

Country	TUNISIA
LOCAL DATA CONTROLLER	**Servier Tunisie**
Registered address	Rue du Lac Huron - Résidence Lac 4 - 1053 Les Berges du Lac - Tunis

Country	TURKEY
LOCAL DATA CONTROLLER	**Servier Ilac Ve Arastirma Anonim Sirketi**
Registered address	Maslak Meydan Sok., Beybi Giz Kule No: 1, Kat: 22-23, Sariyer Istanbul, Turkey

Country	UKRAINE
LOCAL DATA CONTROLLER	Servier Ukraine LLC
Registered address	24, Bulvarno-Kudriavska Street, Kyiv, 01054, Ukraine

Country	UNITED ARAB EMIRATES
LOCAL DATA CONTROLLER	**LLS Representative Office**
Registered address	

Country	UZBEKISTAN
LOCAL DATA CONTROLLER	**LLS Representative Office**
Registered address	

Country	VENZUELA
LOCAL DATA CONTROLLER	**Laboratorios Servier S.A.**
Registered address	Avenida Sanatorio del Ávila Centro Empresarial Ciudad Center, Torre F, piso 3 – Boleíta Norte – Caracas

Country	VIETNAM
LOCAL DATA CONTROLLER	**Servier Vietnam Company Limited**
Registered address	11th Floor, 81-83-83B-85, Ham Nghi Street, Nguyen Thai Binh Ward, District 1, Ho Chi Minh City

3. List of Local Data Protection Officers or Contacts [TO BE LATER PROVIDED]

Country	Local Data Protection Officers	Local Data Protection Contacts
Algeria		
Argentina		
Armenia		
Australia		
Austria		
Azerbaidjan		
Belarus		
Belgium		
Brazil		
Cambodia		
Canada		
China		
Colombia		
Denmark		
Ecuador		
Egypt		

France		
Georgia		
Germany		
Hong Kong		
India		
Indonesia		
Ireland		
Italy		
Ivory Coast		
Japan		
Kazakhstan		
Korea		
Lebanon		
Luxembourg		
Malaysia		
Mexico		
Morroco		
Netherlands		
Nigeria		
Norway		
Pakistan		
Panama		
Peru		
Philippines		
Portugal		
Russia		
Saudi Arabia		
Serbia		

Singapore		
South Africa		
Sri Lanka		
Spain		
Sweden		
Switzerland		
Thailand		
Tunisia		
Turkey		
Ukraine		
United Arab Emirates		
United Kingdom		
Uzbekistan		
Venezuela		
Vietnam		

APPENDIX 3: NATURE AND PURPOSES OF PERSONAL DATA BEING TRANFERRED WITHIN THE SCOPE OF THE BCRs

Purposes of the transfers	**Categories of Data Subjects**	**Categories and nature of the data transferred**	**Recipients in the third country or countries**
► Recruitment	► Candidates, if need be, family environment of candidate	➢ Civil status ➢ Family data ➢ Professional Life ➢ Economic and Financial situation ➢ Education and degrees ➢ Spoken languages	➢
► HR Administration and Payroll Management including: – Training management – Talent management – Internal Directory	► Employees ► Interim workers ► Providers with access to premises, or with regular access to the	► <u>Administrative management of the staff</u>: ➢ Civil status ➢ Family Data ➢ National ID number (Social Security	►

– Occupational medicine. – Working time management – Risk assessment with regard to the exposition of staff to chemical substances – Monitoring of internet use by the staff – Electronic Vote – Cultural and social activities management – Gym access and use management – Whistleblowing scheme	information system (listed in the PIANO directory)	Number) ➢ Professional Life (free zone in PEOPLESOFT, CV and CIVA) ➢ Continuous Training (free zone in PEOPLESOFT, also in a field of CIVA) ➢ Spoken Languages (free zone in PEOPLESOFT, also in a field of CIVA) ► <u>PIANO Directory for external providers</u>: ➢ Civil status (name, surname, phone number, e-mail address) ➢ Location (on site, office) ➢ Professional Life (professional e-mail address, hierarchy)(employees' place of work, type of contract for interims, start and termination of contract) ► <u>Payroll Data</u>: ➢ National ID (Social Security	

		Number) ➢ Bank account information ► <u>Intranet site E-CE – LSI Data</u>: ➢ Civil status ► <u>Management of IT tools supply</u>: ➢ E-mail address ➢ Login data ► <u>Whistleblowing scheme</u> ➢ Identification data (name, email address, phone number, home address, etc.) ➢ Professional Life (job position, CV, education, distinctions, etc.) ➢ Reported facts ➢ Elements gathered in the context of the control of reported allegations	

		➢ The report on the control operations of the reported allegations ➢ Follow-up given to the whistleblowing allegations	
► Network Management	► Network Managers ► Regional Managers ► Medical Sales Representatives by region ► Hospitals Sales Representatives by region ► Medical sales representatives deployed by an external provider, SOFIP	► <u>Calculation of the networks' premiums</u>: ➢ Civil status ➢ Professional Life ➢ Financial situation ► <u>Monitoring of activity and performance assessment of external providers and SERVIER's employees (medical sales and hierarchy)</u>: ➢ Civil status ➢ Professional Life - In the VM depository: business trips, calendars, absences and reason of absence (leaves, sick	►

		leave, long term leave such as maternity), addresses, institutional information; - In MEDESYS: number of contacts, targets objectives, evolution of their market shares in their sector/region, respect of assignments, achievement level of objectives and ranking of medical sales representatives ► <u>Monitoring of the connection to the tracking table of products</u>: ➢ Login data ➢ IP address ➢ Number of connection per period (day/month)	
► Management of Medical Practitioners-oriented	► Health professionals (doctors, pharmacists,	► <u>Management of the Relationship with medical practitioners</u>:	►

Promotion ➢ *Coordination of Promotion Department*	hospital, nurses etc.) ► Medical Sales Representatives ► Other SERVIER employees	➢ Civil status (name and address) ➢ Professional Life (medical specialty, etc.) ➢ Paid medical fees, reimbursement of medical fees (surveys, participation to conferences) ► <u>Targeting of medical practitioners (notably via the ICOMED questionnaire):</u> ➢ Civil status (name, address) ➢ Professional Life (medical specialty, and prescription potential) ➢ Sensitivity to promotional actions ➢ Sensitivity to new technologies (e-Attitude) ➢ Contracts	
► Management of Medical practitioners-oriented Promotion	► Health professionals (participants, speakers)	► <u>CSI SERVICES (Congress Organization)</u>: ➢ Civil status (name, surname, address)	►

➢ *Medical Affairs Department*	► SERVIER employees (medical practitioners attendants) ► Local providers in charge of answering to medical practitioners' needs (Desk)	➢ Professional Life (for medical practitioners: field of work, medical specialty, CV, etc. and the position of medical practitioners in regards to SERVIER: speaker, prescriber, researcher…) ➢ Paid medical fees (surveys, participation to conferences) ► <u>OLYMPE (key opinion leaders)</u>: ➢ Civil status (name, surname, date of birth, title, phone number, deceased "yes/no") ➢ Professional Life: - Public/private sector, in hospital service (yes/no), professional postal address, professional e-mail address, professional phone number, fax number, retired (yes/no),	

		medical specialty, therapeutic field of competence, spoken languages, "regional/national/international awareness", CV; - Information of the leader's attendance to clinical studies operated by SERVIER, participation to conferences or symposiums, attendance to SERVIER Research Institute conferences, memberships to work groups implemented by the Health Authorities, membership to the boards of scientific revues or to learned societies, - Type and dates of contracts	
► Management of Clinical Data	► Patients	► <u>In regards to patients</u>:	►

and of Clinical Studies including: – Case Report Forms completeness and management – Research implementation with regard to several participating health professionals – Participants monitoring – Clinical studies monitoring (selection and monitoring of investigators, patient's files follow-up etc.)	► Investigators ► Supervisors	➢ CRF number, date and place of birth ➢ Number of order (product number, study number, country number, number of the investigator center of the 4 digits of the patient number) ➢ Biological samplings identification (genetic data, for example for pharmacogenomical or biomarkers analyses) ➢ Racial or Ethnical origins, sexual life (contraception) ➢ Health data (pathologies, disease, family medical history, healthcare data, behavioral risks and risk situations) ➢ Personal Life (lifestyle) ➢ Data assessing social difficulties of individuals	

		➢ Deaths (vitality status, and cause of death) ► <u>In regards to medical investigators</u>: ➢ Complete identity (name, surname, professional address, identification logins to the e-CRF, phone details) ➢ Education and Degrees ➢ Compensation and remuneration amounts ➢ Participation in other studies ➢ Professional Life: Professional CV	
► Pharmacovigilance	► Health professionals specialized in surveillance ► Non health professionals (patients, friends, lawyers, etc.)	► <u>Health Professionals</u>: ➢ Surname, name prefix, names ➢ Professional address (city, postal code) ➢ Phone number and telecopy ➢ E-mail address ➢ Medical Specialty	►

		► <u>Patients</u>: ➢ Data likely to be collected: - Health data: family medical history, personal medical history, risk factors, nature and consequences of adverse effects, administered treatments, test results, prescription types, medication uses, therapeutic behavior of prescribers and of health professionals intervening in the management of the disease or of the adverse effect. - Descriptive information: initials, year or date of birth, sex, weight. ➢ Data necessary for the assessment of the adverse effect:	

		- Professional Life: present profession, former professions (only if helpful to assess the cause of the adverse effect) - Tobacco, alcohol and drug consumption - Lifestyle and behavior: dependency (alone, placed in an institution, autonomous, bedridden), assistance (domestic help, family help), physical activity (intensity, frequency, duration), diet and alimentary behavior. ► <u>Others</u>: ➢ Concomitant and suspected drugs ➢ Route of administration ➢ Adverse effects	
► Security and General	► <u>Videosurveillance</u>:	► <u>Videosurveillance</u>:	►

Resources management ➢ *General Services Management*	➢ SERVIER employees ➢ Premises visitors (external providers…) ➢ Clients ► <u>Geo-tracking</u>: ➢ Employees equipped with device ➢ Providers within the firm premises ► <u>Access control:</u> ➢ SERVIER employees ➢ Premises visitors ► <u>Corporate restaurant</u>	➢ Pictures of filmed individuals ► <u>Geo-tracking of isolated workers</u>: ➢ Name, surname of person equipped with device ➢ Location data ➢ Date and hour of events ► <u>Access control</u>: ➢ Name/Surname, company, date and place of birth, type, ID number ➢ Badge number, type of authorized access ➢ Premises accessed by use of badge, inscribed as codes enabling identification of badgers, date and hours of in and out movements. ► <u>Corporate restaurant and vending machine management</u>:	

	and vending machine management: ➢ SERVIER employees Telephony and Conference call management ➢ SERVIER employees ➢ Interim employees ➢ Interns	➢ Badge number ➢ Type of contract ➢ Hierarchy, company ➢ Geographical site, location of the person's desk Telephony and Conference call management ➢ Name, Surname, Phone number ➢ Type of contract ➢ Hierarchy, company ➢ Geographical site, location of the person's desk ➢ Phone number called, service used, operator called, nature of the call (in the form of: local, regional, national, international call), duration, date and time of start and end of call, billing elements (number of charges, the nature and	

		volume of the data exchanged excluding the content of the data and cost of the service used).	
► Risk and General Resources Management ➢ *Industrial Production management*	► <u>Regarding CHEMYS:</u> ➢ Employees of relative entities ➢ Interims ► <u>Regarding POIPOI:</u> ➢ SERVIER employees ➢ Providers	► <u>Regarding CHEMYS (chemical products exposure risk assessment for SERVIER's employees and interims):</u> ➢ Civil status ➢ Social security number ➢ IP address ➢ Professional Life ► <u>Regarding POIPOI (internal Operatonal Plan):</u> ➢ Civil status, related to arrival and departure hour	►
► Commercial Activity and External Communication Management of BIOGARAN	► Clients (contacts in pharmacies) ► Medical Sales Representatives SOFIP	► <u>CRM NEO (information collected by issued questionnaire):</u> ➢ Civil status	►

		► <u>CRM NEO (information collected via the SELLIGENT application):</u> ➢ Civil status (name, surname, sex, date of birth, age) ➢ Professional Life (position, task, date of entry and of exit in pharmacy, number of workers in pharmacy, professionals phone numbers and professional e-mails) ➢ Lifestyle and behavior (hobbies, interests)	
► Finance	► Employees ► Interim workers ► Providers with access to premises, or with regular access to the information system (listed in the PIANO directory)	<u>Management of Business expenditures</u> : ➢ Civil status (name, surname, address, ID card or passport, car registration document) ➢ Professional life (business trips, expenses bills, etc.) ➢ Type of meals	

► Procurement RFP Management	► TO BE COMPLETED	TO BE COMPLETED	
► General Compliance Management – International Coordination – Anti-counterfeiting management – Transparency with regard to relationships with health professionals – Administrative management of patient files – Corporate law management	► TO BE COMPLETED	TO BE COMPLETED	

APPENDIX 4: BCRS INTRA-GROUP AGREEMENT

SERVIER

Binding Corporate Rules (BCRs) for intra-group transfers of Personal Data

[date to be completed]

The following Company(ies) of SERVIER:

Name and address of the relevant BCRs SERVIER Company(ies)

undertake(s) to comply with the provisions of the BCRs of SERVIER.

This undertaking will be relevant for:

- the version dated [to be completed]
  -

- and for any updated BCRs that would be notified according to paragraphs 7.3 and 7.4 of the BCRs

On: _____ (date)
At: _____ (place of signature)

For **SERVIER SAS**	For [name of the relevant **SERVIER Company**]
Name:	Name:
Title:	Title:

► Appendix: see the formal copy of the BCRs attached.