Binding Corporate Rules for Data Protection and Privacy

TABLE OF CONTENTS

1 INTRODUCTION 2
2 DEFINITIONS 2
3 SCOPE 4
4 COMMON PRINCIPLES5
5 DATA SUBJECT RIGHTS 8
6 ACCOUNTABILITY 11
7 SECURITY AND CONFIDENTIALITY 13
8 RESTRICTIONS ON TRANSFERS AND ONWARD TRANSFERS 13
9 TRAINING, COMMUNICATION & AWARENESS 15
10 AUDIT 16
11 COMPLIANCE AND SUPERVISION OF COMPLIANCE 16
12 BCRS NON-COMPLIANCE 17
13 COMPLAINTS HANDLING PROCEDURE 19
14 THIRD PARTY BENEFICIARY RIGHTS 20
15 EEA LIABILITY 21
16 COOPERATION WITH SUPERVISORY AUTHORITIES 21
17 UPDATES OF THESE BCRs 22
18 EFFECTIVE DATE AND TERM OF THE BCRs 22

1 INTRODUCTION

As a global biopharmaceutical company, UCB S.A. and its representation offices and affiliates (collectively, "**UCB**") are engaged in the business of researching, developing, manufacturing, selling and distributing medicinal products to meet the needs of the patients, the healthcare professionals and society as a whole.

To successfully pursue its activities globally, UCB routinely collects, uses, stores, discloses and Transfers across national borders a variety of data, including personal data. To provide a baseline standard for the protection of Personal Data subject to the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**")[1], ePrivacy Directive 2002/58/EC (the "**ePrivacy Directive**")[2] or European Economic Area ("**EEA**")[3] Member State implementing legislation (including the Swiss Federal Act on Data Protection ("**FADP**")[4]), as amended or replaced from time to time, UCB adopted these BCRs, which shall be interpreted in accordance with these laws. In cases where the applicable legislation, for instance national data protection laws, requires a higher level of protection than afforded by these BCRs, it will take precedence over the BCRs.

UCB is committed to ensure the privacy of such Personal Data throughout the world and expects its employees and business partners to take the necessary measures to protect it on behalf of UCB.

As part of its broader privacy compliance and data protection efforts, UCB has included data privacy as one of UCB's core values in its global Code of Conduct and designed a comprehensive privacy and data protection program, with dedicated resources, and has embedded privacy-by-design into its processes and product development, per its Global Policy on the Protection of Personal Data.

In case of a conflict between any UCB internal privacy policies or other related UCB documents, the BCRs shall prevail with regards to Personal Data Transferred subject to the BCRs.

2 DEFINITIONS

- **Binding Corporate Rules** ("**BCRs**") refer to the UCB internal rules detailed in this document (including any of its appendices) to provide appropriate safeguards with regards to Transfers of Personal Data originating in UCB BCRs Entities, subject to the **GDPR**, **ePrivacy Directive** or EEA Member State implementing legislation (including the Swiss **FADP)**, to UCB BCRs Entities located in a Third Country.

- **Competent Supervisory Authority** refers to an EEA supervisory authority competent for monitoring and enforcing compliance of the GDPR by the Data Exporter.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), as amended.
[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended.
[3] EEA Member States: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Republic of Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.
[4] Swiss Federal Act on Data Protection of 25 September 2020, as amended.

- **Controller** refers to a UCB BCRs Entity which alone or jointly with others determines the purposes and means of the Processing Personal Data.

- **Data Exporter** means a UCB BCRs Entity which has Transferred Personal Data, which is subject to the GDPR, to another UCB BCRs Entity in a Third Country.

- **Data Importer** means a UCB BCRs Entity located in a Third Country, to which Data Exporter has Transferred Personal Data, which is subject to the GDPR.

- **Data Protection Officer ("DPO")** refers to the person within UCB who has the overall responsibility for monitoring UCB BCRs Entities compliance with these BCR's, including the trainings and complaint-handling procedure, and supports investigations by Competent Supervisory Authorities, as well as any other specific tasks assigned to it by the relevant data protection laws.

- **Data Subjects** refers to any individuals whose Personal Data are Processed by UCB under these BCRs.

- **Lead Supervisory Authority** refers to the Supervisory Authority competent to act as Lead Supervisory Authority for the cross-border Processing carried out by UCB BCRs Entities. UCB's Lead Supervisory Authority is the Belgian Data Protection Authority.

- **Personal Data** (also known as "Personal Information"). It refers to data directly or indirectly relating to an identified or identifiable natural person (e.g., identifiers such as name, an identification number, address, telephone number, e-mail address, an online identifier etc.).

- **Personal Data Breach** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

- **Processor** refers to a UCB BCRs Entity which Processes Personal Data for or on behalf of the Controller.

- **Processing** refers to any operation or set of operations that are performed upon Personal Data by automatic means or otherwise. This includes the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, disclosure by transmission, dissemination, visual access or making available in any other form, linking, alignment or combination, blocking, erasure or destruction of Personal Data.

- **Special Categories of Personal Data** refer to Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

- **Third Country** refers to a non-EEA country that the European Commission has not deemed to provide an adequate level of data protection, when compared to the EEA.

- **Transfer** refers to the transmission of Personal Data, which is subject to the GDPR, to a Third Country. It includes remote access with the intent to undergo Processing.

- **UCB BCRs Entities** refer to all UCB entities (including branches) listed in Appendix 1 to these BCRs.

- **UCB S.A.** refers to the parent company of the UCB group, established under Belgian law, with registered offices at Allée de la Recherche 60, 1070 Brussels, Belgium, with enterprise number 403.053.608, RPR/RPM Brussels.

Terms not defined in the BCRs shall have the meaning given in the GDPR and/or FADP, as appropriate.

3 SCOPE

- **UCB entities bound by the BCRs:**

The BCRs will be binding on UCB S.A. and all UCB BCRs Entities, as updated from time to time in accordance with the UCB Intra-Group Agreement.

- **Personal Data Processing and Transfers covered by the BCRs:**

These BCRs shall apply to Processing (including Transfers) of Personal Data subject to the GDPR by Data Exporter(s) / Data Importer(s) acting as internal Controller(s)/Processor(s) among UCB BCRs Entities, as well as related onward Transfers of such Personal Data (as outlined in Section 9), for the purposes specified in Appendix 2.

For the avoidance of any doubt, UCB wishes to apply BCRs to Transfers of Personal Data originating from Switzerland/otherwise subject to FADP, in the same manner as the BCRs apply to Personal Data originating from the EEA/otherwise subject to the GDPR. To this end, where these BCRs refer to EEA/GDPR, these references should be understood as including Switzerland/FADP, as appropriate. Swiss Federal Data Protection and Information Commissioner shall also be considered a Competent Supervisory Authority for data protection compliance under the FADP.

- **UCB BCRs Entities compliance with data protection requirements:**

UCB BCRs Entities will ensure an adequate level of data protection of Personal Data Transferred under the BCRs, even where applicable local data protection laws in Third Countries do not meet the standards set out in the BCRs.

Where applicable data protection laws in a Third Country require a higher level of protection for Personal Data than the BCRs, such laws will prevail over these BCRs.

- **UCB employee compliance with the BCRs**

The employees of UCB BCRs Entities may only Process or Transfer (including any onward transfers) Personal Data subject to this BCRs in accordance with these BCRs and relevant local laws and regulations.

Adherence to these BCRs is the responsibility of all UCB BCRs Entities' employees and shall be part of their employment terms and conditions. Any employee of UCB BCRs Entities who breaches these BCRs may be subject to a disciplinary action.

4 COMMON PRINCIPLES

UCB BCRs Entities and their employees shall apply the principles set out below in relation to the Processing of Personal Data described in Appendix 2 which are subject to these BCRs.

- **Transparency and fairness**

  - UCB BCRs Entities provides the following information to the Data Subjects about the Processing of their Personal Data, at the time when their Personal Data is collected from them. This information will be provided in a clear, concise and comprehensive way:

    - The identity and the contact details of the Controller (i.e., the relevant UCB BCRs Entity);
    - The contact details of the Data Protection Officer, where applicable;
    - The purposes and the legal basis for such Processing (if the Processing is based on the legitimate interest pursued by the Controller or by a third party, these interests);
    - The recipients or categories of recipients of the Personal Data, if any;
    - Where applicable, the fact that the Controller intends to transfer Personal Data to a Third Country or international organization and whether there is an adequacy decision by the European Commission in place or if the transfer is based on appropriate safeguards under the GDPR and how a copy of such safeguards can be obtained/accessed.
    - The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
    - Information about Data Subject's rights to request access to, rectify or erase their Personal Data, as well as the right to restrict or object to the Processing, and the right to data portability, as well as the right to lodge a complaint with a Competent Supervisory Authority;
    - Where the Processing is based on consent, the existence of the right to withdraw such consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;
    - Whether the provision of Personal Data is a statutory or contractual requirement / necessary to enter into a contract;
    - Whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide it;
    - The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

  - In addition to the above, the Controller shall provide the Data Subject with the following further information, if their Personal Data have not been collected directly

from them. Controller shall provide this information within a reasonable time 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 used for communication with the Data Subject, at the latest at the time of the first communication to the Data Subject, or, if a disclosure to another recipient is envisaged, at the latest, when the Personal Data are first disclosed.

  - The sources of the Personal Data (including whether they are public);
  - The categories of Personal Data concerned;

- Where the Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data were collected, the Controller shall provide the Data Subject prior to that further Processing with information on that other purpose and with any relevant further information as referred to above.

- The obligation to inform the Data Subject pursuant to this section does not apply to the extent the Data Subject already has this information or, in case the Personal Data has not been obtained from the Data Subject directly if:

  - The provision of such information proves impossible, would involve a disproportionate effort, or is likely to render impossible or seriously impair the achievement of the objectives of the Processing.
  - Obtaining or disclosure is expressly laid down by the applicable EEA or Member State law to which the Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests;
  - Where the Personal Data must remain confidential subject to an obligation of professional secrecy under EEA or Member State law, including a statutory obligation of secrecy.
  - The above information will typically be provided in a form of privacy and data protection policies or other privacy notices, but may take other forms, if appropriate.

- UCB BCRs Entities shall process Personal Data in a fair manner.

- **Purpose limitation**

  - UCB BCRs Entities will Process Personal Data for specified, explicit and lawful purposes in line with Appendix 2 and will not further Process such Personal Data in a manner incompatible with the purposes they were initially Processed for or where otherwise permitted, inform Data Subjects and ensure lawfulness of such processing in line with obligations in these BCRs.

- **Data minimization, accuracy, and storage limitation:**

  - UCB BCRs Entities will limit the Processing of Personal Data to what is adequate, relevant, and necessary in light of the pursued purpose(s). UCB BCRs Entities will not request Data Subjects to provide Personal Data which would not be required to properly fulfil their purposes identified in the BCRs and will stop Processing such Personal Data when it becomes irrelevant to fulfil such purposes. The Processing of such Personal

Data will only be carried out by those UCB BCRs Entity employees/external workers, whose job role(s) and responsibility(s) requires it.

- UCB BCRs Entities will use reasonable means to keep Personal Data accurate, complete, up-to-date and reliable for their intended use. In order to keep the Personal Data accurate and up to date, UCB BCRs Entities have put in place internal processes enabling the Data Subjects to inform them whenever their Personal Data is modified or needs to be updated (in so doing, they also provide access to selfcare tools enabling Data Subjects to amend their Personal Data at their own initiative).

- UCB BCRs Entities will retain Personal Data for only as long as needed to meet the purposes for which the Personal Data was collected and in compliance with UCB's data retention policies and the Global Policy on the Protection of Personal Data, unless otherwise required by applicable EEA laws.

- **Lawfulness**

Processing activities related to Personal Data Processed and Transferred under this BCRs shall be based upon one of the following legal bases:

- the 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; or

- the Processing is necessary for compliance with an EEA/Member State legal obligation to which UCB is subject; or

- the 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 UCB BCRs Entity acting as a Controller; or

- the Processing is necessary for the purposes of legitimate interests pursued by UCB BCRs Entity(s) or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject;

- Data Subject has given their freely given, specific, informed and unambiguous consent; or to protect the vital interests of the Data Subject or another natural person.

- **Processing of Personal Data relating to criminal convictions and offences and related security measures**

The Processing of Personal Data relating to criminal convictions and offences or related security measures under this BCRs based on the above legal bases (see the point on *Lawfulness*) shall only take place under the control of an official authority or when authorized by EEA/Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects. Any comprehensive register of criminal convictions shall be kept only under the control of an official authority.

- **Processing Special Categories of Personal Data**

The Processing of Special Categories of Personal Data Processed and Transferred under this BCRs shall be allowed, if one of the following applies:

- the Data Subject has given his/her explicit consent;

- the Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of UCB BCRs Entities/Data Subject in the field of employment and social security and social protection law in so far as it is authorized by EEA/Member State law or a lawful collective agreement pursuant to EEA/Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;

- the Processing relates to Special Categories of Personal Data which have been made manifestly public by the Data Subject;

- the Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

- the Processing is required 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-care or social care systems and services on the basis of EEA/Member State law or pursuant to contract with a health professional under the obligation of professional secrecy under EEA/Member State law or rules established by national competent bodies or by another person also subject to an equivalent obligation of secrecy;

- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EEA/Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

- the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to appropriate safeguards under and based on EEA/Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

- to protect the vital interests of the Data Subject or another natural person where the Data Subject is physically or legally incapable of giving consent; or

- the Processing is otherwise permitted under EEA/Member State laws.

5 DATA SUBJECT RIGHTS

- **Availability of the BCRs to Data Subjects:**

A version of this BCRs specifically aimed at accessibly informing Data Subjects whose Personal Data is subject to these BCRs will be made publicly available on UCB websites at [add hyperlink]. It will contain at least the following information: Data Subjects' third-party beneficiary rights (including information on the means to exercise those), a description of the scope of the BCRs, and the clauses relating to UCB BCRs Entities' liability, data protection principles, security and Personal Data Breach notifications, restrictions on onward transfers, Data Subjects' rights, list of definitions used, and key practical steps relating to the complaints procedure.

The Data Subjects may also receive a copy of the above upon request, by contacting either the relevant UCB BCRs Entities acting as a Controller, or the DPO, using contact details in a relevant privacy policy/notice.

- **Data Subject Rights**

UCB BCRs Entities shall ensure Data Subjects are provided with the following rights regarding their Personal Data, subject to lawful restrictions:

- To receive **information** related to Processing of their Personal Data (as outlined in the Transparency section above);

- To **access** Personal Data, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing, including receiving a copy of such data;

- To **rectify** inaccurate/complete the incomplete Personal Data about them without undue delay;

- To **erase** Personal Data, if:

  - it is no longer necessary for the purposes for which it has been Processed or Transferred;

  - Data Subject has withdrawn their consent and no other legal ground for Processing exists;

  - Data Subject has objected and no overriding legitimate grounds for the Processing exist;

  - the Processing is unlawful, or erasure is required to comply with a legal obligation.

  The right will not apply if Processing is necessary for:

  - exercising the right of freedom of expression and information;

  - compliance with EEA/Member State law;

  - public interest in the area of public health;

  - archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the appropriate safeguards and in so far as the right

referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that Processing;

- the establishment, exercise or defense of legal claims.

- To **restrict** Processing if:

  - Data Subject contests the accuracy of Personal Data, for a period enabling the Controller to verify the accuracy of the personal data;

  - The Processing is unlawful and Data Subject opposes the erasure and requests the restriction of their use instead;

  - Personal Data is no longer necessary for Processing, but Data Subject requires it for the establishment, exercise or defense of legal claims;

  - Data Subject have objected (see below the right to object) to the Processing, pending the verification by the UCB BCRs Entities whether its legitimate grounds override those of the Data Subject.

  UCB BCRs Entities may store restricted Personal Data and Process it for the establishment, exercise or defense of legal claims/protection of the rights of another person/important public interest or upon the Data Subject's consent.

  UCB BCRs Entities shall inform the Data Subject beforehand in case the restriction is lifted.

- To **data portability**: if the Processing is based on Data Subject's consent or a contract, and is carried out by automated means, Data Subject may request to receive their Personal Data in a structured, commonly used and machine-readable format, and have the right to transmit it to another Controller without hindrance;

- To **object** to Processing, including profiling, if based on performance of a task carried out in the public interest, or based on legitimate interest. In case of objection, UCB BCRs Entities shall no longer process the Personal Data unless it demonstrates a compelling legitimate grounds, which override Data Subject's interests, rights and freedoms or if it is needed for the establishment, exercise or defence of its legal claims.

  Data Subjects may at any time object to direct marketing, including related profiling, and UCB BCRs Entities shall no longer process such Personal Data in that context;

- **Not to be subject to** decisions based solely on **automated Processing**, including profiling, which produces legal or similarly significant effects concerning the Data Subject, unless this is *a)* necessary for entering into, or performance of, a contract, or *b)* subject to the Data Subject's explicit consent or *c)* authorized by EEA/Member State law. Such decisions shall not be based on Special Categories of Personal Data, save for the Processing of such data being based on Data Subject's explicit consent or being necessary for reasons of substantial public interest under EEA/Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place. To the extent *a)* or *b)* apply, the Controller will implement suitable measures to safeguard the Data Subject's rights and freedoms and

legitimate interests, at least the right to obtain human intervention on the part of the Controller, to express his or her point of view and to contest the decision.

UCB BCRs Entities shall communicate any rectification or erasure of Personal Data or restriction of Processing to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. UCB BCRs Entities shall inform the Data Subject about those recipients upon request.

To exercise the above rights, Data Subjects may contact UCB BCRs Entities acting as Controllers directly, or alternatively contact the DPO by letter at UCB S.A. or by email to datasubjectrequests@ucb.com.

Employees of UCB BCRs Entities may request access and modifications to their Personal Data via our internal platform (HRAnswers) or by sending a written request, by letter or email, to the local Human Resources Department.

UCB BCRs Entities will implement suitable measures to protect the Data Subject right(s) described above. They will respond to Data Subjects' requests related to their rights under these BCRs without undue delay and in any event within one (1) month of receipt of the request. If, due to the complexity and/or number of the request the relevant UCB BCRs Entity cannot respond within this time, it may extend it by two (2) months, as necessary. within one (1) month. In such cases, it will notify the Data Subject of the extension and reasons for the delay within one (1) month of the receipt of the request. If the relevant UCB BCRs Entity does not intend to respond to the request, it will inform the Data Subject of its reasons for not doing so and their right to lodge a complaint with a Competent Supervisory Authority and seek a judicial remedy, within one (1) month of the receipt of the request. Where requests from a Data Subject are manifestly unfounded or excessive, relevant UCB BCRs Entity may charge a reasonable fee, or refuse to act on the request.

6 ACCOUNTABILITY

Each UCB BCRs Entity is responsible for its compliance with the BCRs. In order to demonstrate compliance, UCB BCRs Entities shall, as applicable:

- maintain a written record, including in electronic form, of Processing activities, subject to the GDPR and these BCRs, and make it available to the Competent Supervisory Authorities on request.

  For Controller UCB BCRs Entities, it shall contain the following in relation to Personal Data:

  - the name and contact details of the Controller and, where applicable, the joint Controller and the DPO;
  - the purposes of the Processing;
  - a description of the categories of Data Subjects and of the categories of Personal Data;
  - the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in Third Countries/international organizations;

- where applicable, transfers of Personal Data to a Third Country/international organization, including the identification of that Third Country or international organization and the documentation of suitable safeguards, as applicable;

- where possible, the envisaged time limits for erasure of the different categories of Personal Data;

- where possible, a general description of applied technical and organizational security measures.

For Processor UCB BCRs Entities, it shall contain the following in relation to Personal Data:

- the name and contact details of the Processor and each Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or the Processor's representative, and the DPO;

- the categories of Processing carried out on behalf of each Controller;

- where applicable, transfers of Personal Data to a Third Country/international organization, including the identification of that Third Country or international organization and the documentation of suitable safeguards, as applicable.

- Taking into account the nature, scope, context and purposes of the Processing subject to the BCRs, perform privacy risks assessments, including data protection impact assessments ("**DPIA**") for the Processing that is likely to result in a high risk to the rights and freedoms of Data Subjects, in particular where it involves:

  - A systematic and extensive evaluation of personal aspects relating to Data Subjects based on automated processing (including profiling), which produces legal or similarly significant effects on the Data Subject;

  - Large-scale Processing of Special Categories of Personal Data; or

  - Large-scale systematic monitoring of a publicly accessible area.

  The DPIA shall contain the following:

  - A systematic description of the envisaged Processing and its purposes;

  - An assessment of the necessity and proportionality of the Processing in relation to the purposes;

  - An assessment of the risks to the privacy rights and freedoms of Data Subjects;

  - Measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and demonstrate compliance with applicable EEA data protection laws.

  Relevant UCB BCRs Entities performing the assessment shall ask the DPO for advice in connection with the assessment.

The Competent Supervisory Authorities shall be consulted prior to Processing where a DPIA indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk.

- Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing, the Controller UCB BCRs Entities shall, both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organizational measures designed to implement and ensure compliance with data protection principles by design and by default.

7 SECURITY AND CONFIDENTIALITY

UCB BCRs Entities will establish and maintain security policies providing for appropriate administrative, technical, and physical measures to safeguard and appropriately protect Personal Data from unauthorized use, disclosure, destruction, and alteration, in particular where the Processing involves the transmission of data over a network. These security measures shall be updated regularly to take into account the state of the art and will be commensurate with the risks associated with the types of Processing and the nature of the Personal Data covered by these BCRs, and related implementation cost. Considering their risk profile, Special Categories of Personal Data might require varying protective measures.

Employees are instructed to notify to UCB, via a specific mailbox, any Personal Data Breach of which they become aware. The UCB BCRs Entity that has suffered a Personal Data Breach will notify it to UCB S.A. and the DPO without undue delay. Where relevant, if a UCB BCRs Entity acts as a Processor, it will also notify the relevant UCB BCRs Entity acting as a Controller for the affected Personal Data without undue delay.

The affected UCB BCRs Entity (Controller), will also notify, without undue delay, and, where feasible, not later than 72 hours after having become aware of the Personal Data Breach, to the Competent Supervisory Authorities, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of Data Subjects. In cases where such Personal Data Breach is likely to result in a high risk to the rights and freedoms of Data Subjects, they shall be notified by the affected UCB BCRs Entity (Controller) without undue delay.

Furthermore, the Global Privacy Team is responsible for documenting any Personal Data Breaches. Such documentation shall include the facts relating to the Personal Data Breach, its effects and the remedial action taken and shall be made available to the Competent Supervisory Authorities on request.

8 RESTRICTIONS ON TRANSFERS AND ONWARD TRANSFERS

- If UCB BCRs Entities use Processors to Process Personal Data which are subject to these BCRs on their behalf, the UCB BCRs Entities will conclude a written agreement with such Processors. In line with the below, such Processors shall be obliged to:

  - only act on documented instructions of the UCB BCRs Entities (including with regard to (onward) transfers of Personal Data disclosed by UCB BCRs Entities to a Third Country or an international organization);

- have in place sufficient technical and organizational security measures to safeguard the Personal Data disclosed by the UCB BCRs Entity that are appropriate having regard to the risks associated with the types of Processing, the nature of the Personal Data involved and related implementation costs;

- ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- respect the below conditions for engaging another Processor;

    • do not engage another Processor without prior specific or general written authorization of the relevant Controller UCB BCRs Entity. In the case of general written authorization, the Processor shall inform the Controller UCB BCRs Entity of any intended changes concerning the addition or replacement of other Processors to give the Controller UCB BCRs Entity the opportunity to object to such changes;

    • impose the same data protection obligations as set out in the contract or other legal act between the Controller UCB BCRs Entity and the Processor itself, including ensuring that where that other Processor fails to fulfil its data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of that other Processor's obligations;

- assist the Controller UCB BCRs Entity by appropriate technical and organizational measures, insofar as this is possible with the fulfilment of its Controller obligation to respond to Data Subject's Rights requests;

- assist the Controller UCB BCRs Entity with ensuring compliance with the security of processing, notification requirements both to the Competent Supervisory Authorities and Data Subjects in case of a Personal Data Breach, data protection impact assessments and prior consultations with the Competent Supervisory Authority, taking into account the nature of Processing and the information available to the Processor;

- delete or return to the Controller UCB BCRs Entity, at their choice, all Personal Data after the end of the provision of services relating to Processing, and delete existing copies, unless EEA/Member State law requires otherwise;

- make available to the Controller UCB BCRs Entity all information necessary to demonstrate compliance with its legal obligations and contribute to audits, including inspections, conducted by the Controller/external auditor mandated by the Controller. The Processor shall immediately inform the Controller UCB BCRs Entity if, in its option, an instruction infringes the GDPR or EEA/Member State laws.

▪ In addition to the above UCB BCRs Entities will only onward transfer Personal Data subject to the BCRs to external processors or controllers that are located in Third Countries/international organizations, after ensuring an adequate level of protection for such Personal Data in line with the GDPR, including supplemental measures, as appropriate. In particular, base such onward transfers on appropriate safeguards, including approved:

    • Approved Processor binding corporate rules;

    • Standard contractual clauses adopted/approved by the European Commission; or

- Approved code of conduct or certification mechanism adhered to by the Recipient.

Data Importers will assess whether the recipient processor/controller/third party/international organization is subject to any legal requirements under Third Country laws, which are likely to have a substantial adverse effect on the guarantees provided by the above safeguards. Where necessary, Data Importer shall identify and implement appropriate supplementary measures, to ensure its findings are appropriately addressed, or consider not carrying out such onward transfers.

Where such onward transfers cannot be based on the above safeguards, it may take place based on one of the following derogations:

- Explicit consent of the Data Subject, after having been informed appropriately about the potential risks;

- It is necessary for the performance of a contract between the Data Subject and the Data Importer / implementation of related pre-contractual arrangements taken at the Data Subject's request / performance of a contract concluded in the interest of the Data Subject between the Data Importer and another natural or legal person;

- It is necessary for important reasons of public interest under EEA/Member State laws;

- It is necessary for the establishment, exercise or defence of legal claims;

- It 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;

- It is made from a register which according to EEA/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 a legitimate interest, but only to the extent that the conditions laid down by EEA/Member State law for consultation are fulfilled in the particular case;

- Provided it is not repetitive and only concerns a limited number of Data Subjects and is necessary for the purposes of compelling legitimate interests pursued by the Data Importer which are not overridden by the interests or rights and freedoms of the Data Subject, and the Competent Supervisory Authority has been informed of such transfer.

9 TRAINING, COMMUNICATION & AWARENESS

All employees of UCB BCRs Entities, who have regular access to Personal Data in their day-to-day activities, such as development of related IT tools/processes, conduct of clinical trials, marketing, management of employees and other human resources, etc. will be regularly (at least annually) provided, with appropriate awareness and training materials on these BCRs (including management of Requests as outlined in Section 12 below) and data protection rules in general.

A series of communication will be issued, and awareness campaigns will be launched on a regular basis, in collaboration with other key stakeholders contributing to the privacy and data protection such as cybersecurity and our human resources department. Together with fact

sheets and other FAQs, this will contribute to increased employee awareness and sensitivity to privacy and data protection requirements.

10 AUDIT

The Global Internal Audit Department of UCB shall evaluate and report to the Audit Committee and the Board of Directors, in coordination with the Global Privacy Team, on all aspects of the BCRs, such as the IT systems (incl. applications, databases) that process Personal Data subject to BCRs, onward transfers, decisions taken as regards mandatory requirements under national laws that conflict with these BCRs, review of the contractual terms used for the transfers to controllers or processors of Personal Data outside of UCB BCRs Entities, corrective actions, etc. s on a periodic basis.

Audits will be carried out annually and their frequency and main focus may be adjusted by UCB BCRs Entities in the light of the risks to the rights and freedoms of Data Subjects posed by the Processing. Audits of compliance with the BCRs may be undertaken by external auditors, if UCB so decides.

The results of the audit will be reported by Global Internal Audit to the DPO and UCB S.A.'s Board of Directors through the Audit Committee, which will evaluate that procedures are in place to ensure that any necessary corrective action takes place as soon as reasonably practicable.

In addition to such regular audits, DPO and UCB S.A.'s Board of Directors may request the Audit Committee to instruct the Global Internal Audit Department of UCB or an external auditor to carry out a specific (ad hoc) audit

Where any non-compliance with the BCRs is identified during the audits, the auditors will work with the relevant UCB BCRs Entities to assist them in developing and implementing remediation measures. The audit team will periodically monitor the progress of the remediation plans.

If requested by a Competent Supervisory Authority, the Global Internal Audit Department will also provide a copy of the results of the audit to such Competent Supervisory Authority, subject to applicable laws. Furthermore, a Competent Supervisory Authority shall be given a power to carry out an audit and an inspection of any of UCB BCRs Entities and such UCB BCRs Entities shall accept to be audited and to be inspected by such relevant Competent Supervisory Authority.

11 COMPLIANCE AND SUPERVISION OF COMPLIANCE

The UCB's privacy program includes an appropriate governance mechanism and body to ensure compliance and supervision of compliance with the UCB BCRs. It includes the following resources:

- **Global Privacy Team**

The UCB Global Digital & Data Privacy Center of Excellence oversees the UCB privacy program and ensures UCB BCRs Entities' compliance with the BCRs. The team is led by the Associate General Counsel, Head of Legal Digital Technology, IT and Data Privacy ("**AGC DDP**"), responsible for overseeing and enabling day-to-day compliance with the BCRs at a regional and global compliance level. The AGC DDP is further supported by a dedicated team,

located in the EU and US (altogether "**Global Privacy Team**"). The Global Privacy Team serves as an escalation structure for all teams with privacy functions at UCB and drives consistency across the organization.

The AGC DDP regularly reports and advises on compliance with BCRs on a global level to the Head of Ethics & Legal Affairs, General Counsel, who include relevant information in their regular reporting to the Board of Directors.

- **Global Data Protection Officer**

UCB has appointed a Global DPO, who is in the context of these BCRs, responsible for monitoring compliance with the BCRs, including relevant trainings and complaint-handling procedure and supports investigations by Competent Supervisory Authorities. The Global Privacy Team, the Privacy Champions, the Global Internal Audit and the Ethics & Legal Affairs teams cooperate with the DPO, as appropriate. The DPO reports dotted line into the UCB General Counsel.

- **Data Privacy Council**

The UCB Data Privacy Council is a forum where key stakeholders who can drive and guarantee an adequate level of compliance for our privacy program, including the BCRs, meet regularly (and *ad hoc*, if required). Besides the AGC DDP and the DPO, such key stakeholders will represent the following departments: human resources, IT & Cybersecurity, Procurement, Research & Development, Ethics & Legal Affairs, Marketing, Global Internal Audit and additional subject matter experts, as required.

- **Ethics & Legal Affairs**

The UCB network of Ethics & Compliance Officers is widely spread across the organization and is therefore perfectly suited to provide basic training and create awareness for all employees, in particular newcomers. Based on their roles and positions, they contribute to distil and relay information across the different UCB BCRs Entities.

The UCB Legal Affairs department serves as a first line of support for the UCB teams for any privacy and data protection aspects, including legal advising and contracts reviews.

- **Privacy Champions**

To guarantee an adequate level of support to the UCB teams but also to ensure appropriate compliance with our BCRs, the Global Privacy Team has implemented a network of Privacy Champions to cover specific departments such as human resources, research & development, etc. The Privacy Champions actively support the different teams and help the Global Privacy Team to create awareness and train our UCB workforce, as well as relay the information upwards to the Global Privacy Team.

12 BCRS NON-COMPLIANCE

This section outlines UCB BCRs Entities commitments with regards to prior assessment of Third Country laws and practices affecting BCRs compliance, response to a legally binding public authority ("**Requesting Authority**") request for access to Personal Data subject to the BCRs ("**Request**"), or such direct access by Requesting Authority ("**Access**"), without prior

interaction with UCB BCRs Entities (e.g., during the transit between Data Exporter and Importer), as well as the applicable limitations and safeguards.

- **Prior assessment**

Prior to UCB BCRs Entities transferring Personal Data subject to BCRs, they will assess whether laws and practices of Third Countries where the Data Importer is located may prevent them from complying with BCRs, including those requiring disclosure in response to Requests, and authorizing Access. Any laws and practices that respect the essence of the fundamental rights and freedoms, limit Requests/Access to what is necessary and proportionate in a democratic society, are not in contradiction with the BCR.

The AGC DDP and Global Privacy Team, supported by the Legal Affairs' team is undertaking to document assessments of these laws, as well as the supplementary measures selected and implemented. Such assessments and selected and implemented supplementary measures shall consider specific circumstances of the (onward) Transfer, including purposes of Processing, entities involved, applicable economic sector, categories and format of Personal Data Transferred, location of Processing, including storage, and relevant contractual, technical or organizational safeguards put in place to supplement the BCRs, including measures applied during the transmission and to the processing of the personal data in the country of destination. Documentation will be made available to Competent Supervisory Authority upon request.

Data Exporter(s) (together with Data Importers, as appropriate) will monitor developments in the Third Countries to which they have transferred Personal Data that could affect the initial prior assessment of the level of protection and the resulting Personal Data Transfer decisions, on an ongoing basis.

- **Request and Access**

If the Data Importer receives a Request under local Third Country laws, it will notify Data Exporter and where reasonably possible Data Subjects, about the Personal Data requested, the Requesting Authority, the legal basis for the Request and the response provided. If Data Importer becomes aware of Access, it will provide the above notification and include relevant available information.

If the Data Importer is prohibited from notifying Data Exporter/Data Subjects, it will attempt to obtain a waiver of such prohibition and notify later with a view to communicate the most relevant information possible (including the prohibition itself), when this becomes possible.

The Data Importer will provide the above information it provides to Data Exporter/Data Subjects, to Competent Supervisory Authority upon request.

The Data Importer will preserve the abovementioned information for as long as the Personal Data are subject to the safeguards provided by the BCR.

The Data Importer will review the legality of the Request (including vis-à-vis the lawful powers of the Requesting Authority) and make reasonable efforts to challenge the Request if, after careful assessment, it concludes that there are reasonable grounds to consider that the Request is unlawful under applicable Third Country laws, international law, and principles of international comity. Data Importer will consider pursuing possibility of an appeal, including seeking interim measures to suspend the Request, until competent judicial authority has

decided on its merits. It will not disclose Requested Personal Data until required to do so under the applicable procedural rules.

The Data Importer will document any prohibitions outlined above, its related assessments and efforts, and to the extent permissible under applicable Third Country laws, make them available to the Data Exporter and Competent Authority upon request.

If in the above cases Data Importer is not in a position to notify the Competent Supervisory Authorities/ Data Subjects/ Data Exporter it shall provide general information on the Requests/Access to the Competent Supervisory Authorities (e.g., a number of Requests for disclosure, type of data requested, Requesting Authority, if possible, etc.) on an annual basis.

The Data Importer will provide the minimum amount of information permissible when responding to a Request, based on its reasonable interpretation.

As a general rule, UCB BCRs Entities shall ensure that any Personal Data Transfer(s) to any public authority is not massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

- **Consequences of the inability to comply with BCRs**

If a Data Importer discovers, or Data Exporter believes that Data Importer has become subject to laws (including legislation they monitor)/measures (e.g., unlawful Request/Access)/practices preventing it from/is unable to comply with the BCRs, it must promptly notify UCB S.A., the Global Privacy Team and Data Exporter. Data Exporter, UCB S.A. and the Global Privacy Team will identify any available supplementary measures that Data Exporter/Importer can adopt to fulfil their obligations under the BCRs.

If no adequate supplementary measures are available and Data Importer is still unable to comply with BCRs, or if instructed by the Competent Supervisory Authority, Data Exporter should suspend the relevant Transfer (and other Transfers for which the assessment would have the same result). UCB S.A. and the Global Privacy Team will notify other UCB BCRs Entities about the result, to allow them to apply identified supplementary measures/need for suspension of Transfers, as appropriate.

If suspension 1) cannot be lifted within one month due to persistent breach, 2) or Data Importer is in substantial breach of the BCRs, or 3) it fails to comply with a binding decision of competent court or Competent Supervisory Authority regarding its compliance with BCRs, it shall, at the choice of Data Exporter, return/delete such Personal Data (and its copies) it received under the BCRs.

Data Importer shall ensure continued compliance with BCRs until such Personal Data is returned/deleted, including where local Third Country laws prohibit return/deletion, and not Process Personal Data beyond what is required by such laws. Data Importer will certify the deletion to Data Exporter once complete.

13 COMPLAINTS HANDLING PROCEDURE

- **UCB complaints handling procedure:**

Any Data Subject (including UCB employees) who believes their Personal Data may have been Processed in violation of these BCRs by any UCB BCRs Entity, may submit his/her complaint

by mail or by email to the Global Privacy Team email address at dataprivacy@ucb.com or to the postal address of UCB S.A. (letter addressed to the Global Privacy Team to ensure timely processing), or orally to a member of the Global Privacy Team, if requested. In case the Data Subject is a UCB employee, the request can also be made through the internal platform (HRAnswers).

The complaint must identify the UCB BCRs Entity(s) concerned and describe the alleged breach of the BCRs in as much detail as possible and must be accompanied by all relevant documents and evidence.

The Global Privacy Team will coordinate response with the relevant UCB BCRs Entity. Except in exceptional circumstances, relevant UCB BCRs Entity, will send acknowledgment of receipt of a complaint to the Data Subject within ten (10) working days.

The Global Privacy Team may at their discretion consult the DPO, where appropriate, in particular where the complaint is to be rejected.

Relevant UCB BCRs Entity, supported by Global Privacy Team will investigate and provide a substantive response to the complaint without undue delay, but no later than one (1) month after receiving the complaint. Such decision is provided by mail, email or orally to the Data Subject, as appropriate.

If, due to the complexity and/or number of the complaints, relevant UCB BCRs Entity, supported by the Global Privacy Team cannot provide a substantive response within one (1) month, it will notify the individual who made the complaint of an extension within one month of the receipt of the request, together with the reasons for the delay and provide a reasonable estimate of the timeframe (not exceeding two (2) further months) within which a response will be provided.

If the complaint of the Data Subject cannot be satisfied, UCB BCRs Entity will justify such refusal and provide relevant reasons in its response to the Data Subject and inform them of the possibility to lodge a complaint with a Competent Supervisory Authority and seek a judicial remedy, which Data Subject has at all times during the complaints procedure.

- **Additional reporting obligations for employees of UCB BCRs Entities:**

Any employee of UCB who has reasons to believe these BCRs have been violated shall contact his/her immediate manager, or the Global Privacy Team.

Violations or suspected violations of these BCRs may also be reported using UCB's compliance reporting systems, e.g. the UCB Integrity Line.

14 THIRD PARTY BENEFICIARY RIGHTS

Data Subjects whose Personal Data is (i) subject to the GDPR and (ii) Transferred to UCB BCRs Entities outside of the EEA under these BCRs shall have the right to enforce the rules provided in Sections 4, 5, 6, 7, 8, 9, 12, 13, 14, 15, 16 and 17 of these BCRs as third-party beneficiaries of the BCRs for Personal Data detailed in Appendix 2 and as specified below right to seek judicial remedy and redress, including the payment of compensation, arising from a breach of the enforceable elements of the BCRs. In such instances, Data Subjects may be represented by a not-for-profit body, organization or association which has been

properly constituted in accordance with the law of an EEA Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of Data Subjects' rights and freedoms.

The Data Subjects whose Personal Data has been Transferred to UCB BCRs Entities located outside of the EEA subject to these BCRs will have the right to lodge a complaint, at their option, with:

(i) the Competent Supervisory Authority in the EEA Member State of the Data Subject's habitual residence, place of work or place of the alleged infringement; or

(ii) the competent courts of the EEA Member State where the UCB BCRs Entity acting as a Controller or Processor has an establishment or where the Data Subject has their habitual residence.

15 EEA LIABILITY

- **UCB BCRs Entity within the EEA**

Each UCB BCRs Entity within the EEA shall bear the sole responsibility for any violation of Sections 4, 5, 6, 7, 8, 9,13, 14, 15, 16 and 17 of these BCRs within the EEA, to the extent provided under the GDPR.

If UCB BCRs Entity demonstrates that it is not liable for the violation resulting in damages claimed, it may discharge itself from such liability.

- **UCB BCRs Entity outside the EEA**

For Personal Data originating from the EEA/otherwise subject to the GDPR and Transferred outside the EEA under these BCRs, UCB S.A. will be liable and accept to remedy the acts of any UCB BCRs Entity located outside of the EEA and to pay compensation for any material or non-material damages a Data Subject may suffer due to a breach of these BCRs caused by such non-EEA UCB BCRs Entity to the extent ordered by courts and/or Competent Supervisory Authorities. In such cases, relevant courts/other judicial authorities in the EEA will have jurisdiction, and Data Subjects will have the rights and remedies against UCB S.A., as if the violation had been caused by the latter in Belgium.

In case the Data Subjects can demonstrate that they have suffered such damages and establish facts that show that it is likely that the damages have occurred because of a breach of the BCRs, it shall be for UCB S.A. to prove that it or the relevant non-EEA UCB BCRs Entity was not responsible for the breach of the BCRs giving rise to those damages or that no such breach took place.

16 COOPERATION WITH SUPERVISORY AUTHORITIES

The UCB BCRs Entities shall agree to cooperate with the Competent Supervisory Authorities, including by providing the Competent Supervisory Authorities with any information about the processing operations covered by the BCR, accounting for their advice, and by abiding by their decisions, regarding matters related to these BCRs.

The UCB BCRs Entities also undertake to respond within a reasonable timeframe to requests the Competent Supervisory Authorities may make regarding these BCRs, including audit and inspection requests (including on-site, where necessary).

Any dispute related to the exercise of supervision of compliance with the BCRs by Competent Supervisory Authority will be resolved by the courts of the EEA Member State of that Competent Supervisory Authority, in accordance with that EEA Member State's procedural law. The UCB BCRs Entities agree to submit to the jurisdiction of those courts.

17 UPDATES OF THESE BCRs

UCB BCRs Entities assisted by the Global Privacy Team are responsible for keeping these BCRs up-to-date, and in compliance with the GDPR and applicable Recommendations issued by the European Data Protection Board.

UCB S.A. will notify all UCB BCRs Entities of any modifications to these BCRs, including the list of UCB BCRs Entities, without undue delay.

UCB S.A. will provide information about such modifications (including to confirm no modifications were made) to Lead Supervisory Authority at least once a year, with a brief explanation of the reasons for the changes. This annual communication should also include the renewal of the confirmation that UCB S.A. has sufficient assets or has made appropriate arrangements to enable itself to pay compensation for damages resulting from a breach of the BCRs. Where a BCRs modification would possibly be detrimental to the level of the protection offered by the BCRs or significantly affect the BCRs, it shall be communicated to the Lead Supervisory Authority in advance, with a brief explanation of the reasons for the modification, and the Lead Supervisory Authority will also assess whether the changes made require a new approval.

The Global Privacy Team is responsible for keeping the updated copy of the BCRs as well as the list of UCB BCRs Entities and recording of any modifications. It shall make these available upon request to Competent Supervisory Authorities and providing relevant updates regarding such modifications to Data Subjects.

No Transfer of Personal Data can take place until UCB BCRs Entity is effectively bound by the BCRs and can deliver compliance with the BCRs.

18 EFFECTIVE DATE AND TERM OF THE BCRs

The BCRs shall become effective for all the UCB BCRs Entities upon the execution of an intra-group agreement by the UCB BCRs Entities. In those countries where the applicable law requires the approval by local authorities and/or the completion of other formalities before the BCRs can become effective, the BCRs will only become effective in such countries upon receipt of the relevant approval and/or completion of the relevant formalities.

The BCRs shall remain in force for an indefinite period of time.

In the event of termination of the above-mentioned intra-group agreement by any of the UCB BCRs Entities, the BCRs shall cease to be binding and enforceable upon such UCB BCRs Entity for all Personal Data Processed or Transferred after the date of termination. The obligations derived from the BCRs for Personal Data Transferred subject to the BCRs up until termination, shall remain until these Personal Data have been erased or as long as and to the extent required

by applicable laws and regulations. In the event of such change, the UCB BCRs Entity responsible for the administration of the intra-group agreement will take any required steps to update the BCRs, in accordance with the provisions of Section 17.

If the Data Exporter and Data Importer agree that the Personal Data Transferred subject to the BCRs prior to the termination may be kept by the Data Importer following the termination (as outlined above), their protection must be maintained in accordance with Chapter V of the GDPR, otherwise Data Importer shall erase such Personal Data.

Appendix 1 – UCB BCRs Entities

AUSTRALIA
Engage Therapeutics Australia Pty. Ltd., Level 1, 1155 Malvern Road – 3144 Malvern, Victoria (ACN 629 777 555)
UCB Australia Pty. Ltd. – Level 1, 1155 Malvern Road – 3144 Malvern, Victoria (ACN 005 799 208)

AUSTRIA
UCB Pharma Gesellschaft m.b.H. – Twin Tower, Wienerbergstrasse 11/12a, 1110 Wien (Register FN 60360 s | VAT ATU14257301)

BELGIUM
Sifar SA – Allée de la Recherche, 60 – 1070 Brussels (BE0453.612.580)
UCB Belgium SA – Allée de la Recherche, 60 – 1070 Brussels (BE0402.040.254)
UCB Biopharma SPRL – Allée de la Recherche, 60 – 1070 Brussels (BE0543.573.053)
UCB Fipar SA – Allée de la Recherche, 60 – 1070 Brussels (BE0403.198.811)
UCB Pharma SA – Allée de la Recherche, 60 – 1070 Brussels (BE0403.096.168)
UCB Ventures Belgium SA – Allée de la Recherche, 60 – 1070 Brussels (BE0668 388 891)
UCB Ventures SA – Allée de la Recherche, 60 – 1070 Brussels (BE0667 816 096)

BRAZIL
UCB Biopharma Ltda – Avenida Presidente Juscelino Kubitschek, nº 1327, 5° andar, Condominio Edificio Intemacional Plaza II, CEP : 04543-011 São Paulo (Register 64.711.500 / 0001-14 | 35.209.754.931)

BULGARIA
UCB Bulgaria EOOD – 2B Srebarna street, fl. 9, office 8B, Lozeneth, Sofia 1407 (Register 200315158 | VAT BG200315158)

CANADA
UCB Canada Inc. – 2201 Bristol Circle, Suite 602, Oakville, Ontario L6H 0J8 (Register 664246-2)

CHINA
UCB Pharma (Hong Kong) Ltd – Rooms 156 & 157, 20/F, Cityplaza Three, 14 Taikoo Wan Road, Tai Koo, Hong Kong (Register 596833)
UCB Pharma (Zhuhai) Company Ltd – Section A., Workshop, No.3 Science & Technology 05th Road, Innovation Coast, National Hi-Tech Industrial Development Zone – Zhuhai Guangdong Province (Register440402632815726)
UCB Trading (Shanghai) Co Ltd – Suite 317, 439 No.1 Fu Te Road West, Shanghai (Pilot Free Trade Zone) (Register 310115400192973)

CZECH REPUBLIC
UCB S.R.O. – Jankovcova 1518/ 2 – 170 00 Praha 7 (C 17194 (Identification Number 457 86 950 | VAT CZ45786950)

DENMARK
UCB Nordic AS – Edvard Thomsens Vej 14, 7 – 2300 Copenhagen (Register 26 68 89 49 | VAT DK 26 68 89 49)

FINLAND
UCB Pharma Oy Finland – Bertel Jungin aukio 5, 6.krs – 02600 Espoo (Register 0114461-2 | VAT FI01144612)

FRANCE
UCB Pharma SA – Défense Ouest 420, rue d'Estienne d'Orves – 92700 Colombes (Register 562 079 046 | VAT FR14 562 079 046)

GERMANY
Cosmix Verwaltungs GmbH – Rolf-Schwarz-Schütte Platz 1 – 40789 Monheim am Rhein
UCB BioSciences GmbH – Rolf-Schwarz-Schütte Platz 1 – 40789 Monheim (Register Düsseldorf 46849 | VAT DE813201746)
UCB GmbH – Rolf-Schwarz-Schütte Platz 1 – 40789 Monheim (Register Düsseldorf 58429 | VAT DE121862092)
UCB Pharma GmbH – Rolf-Schwarz-Schütte Platz 1 – 40789 Monheim (Register Düsseldorf 62600 | VAT DE121395506)

GREECE
UCB A.E. – 63 Agiou Dimitriou Street – 17456 Alimos – Athens (Register 4892/01/NT/86/179(99) | VAT GR094 125 994)

HUNGARY
UCB Hungary Ltd – Obuda Gate Building Arpád Fejedelem ùtja 26-28 – 1023 Budapest (Register 01-09-076436 | VAT HU10547085)

INDIA
UCB India Private Ltd – Building No. - P3, Unit No. - 103, 1st Floor, Prithvi Complex, Kalher Pipe Line, Kalher, Bhiwandi, Thane, Maharashtra 421302 (Register 11545 CIN: U24239MH1959PTC011545)

IRELAND
UCB (Pharma) Ireland Ltd – United Drug House Magna Drive, Magna Business Park, City West Road – Dublin 24 (Register 226881 | VAT IE8226881Q)
UCB Manufacturing Ireland Ltd – United Drug House Magna Drive, Magna Business Park, City West Road – Dublin 24
Zogenix ROI Limited – United Drug House Magna Drive, Magna Business Park, City West Road – Dublin 24

ITALY
UCB Pharma SpA – Via Varesina 162 – 20166 Milano (Register MI -1857523 | VAT IT 00471770016)

JAPAN
UCB Japan Co Ltd – Shinjuku Grand Tower, 8-17-1 Nishi-Shinjuku 160-0023 Shinjuku, Tokyo (Register 0111-01-063273)

MEXICO
UCB de Mexico SA de C.V. – Calzada Mariano Escobedo 595, Piso 3, Oficina 03/100, Colonia Rincón del Bosque, Bosque de Chapultepec I sección, Alcaldía Miguel Hidalgo – C.P.11589 City of Mexico (Register 196876 | Tax ID UME9702128Z3)

NETHERLANDS
UCB Pharma B.V. (Netherlands) – Hoge Mosten 2 – 4822 NH Breda (Register 20049189 | VAT NL007411765B05)

NORWAY
UCB Pharma A.S. – Haakon VIIs gate 6, 06161 Oslo, Norway (Register 976 281 918 | VAT NO976281918)

POLAND
UCB Pharma Sp. z.o.o. – ul. L. Kruczkowskiego 8 – 00 380 Warszawa (Register 118263 | VAT PL5261020151)
Vedim Sp. z.o.o. – ul. L. Kruczkowskiego 8 – 00 380 Warszawa (Register 129531 | VAT PL1230969455)

PORTUGAL
UCB Pharma (Produtos Farmaceuticos) Lda – Rua do Silval, nº 37, piso 1, S1.3, 2780-373 Oeiras (Register 500291322 | VAT PT 500 291 322)

ROMANIA
UCB Pharma Romania S.R.L. 165 Calea Floreasca, One Tower Building, 3rd Floor, 1st district, Bucharest 14459 (Register J40/18836/2008 | Sole registration code: 24708161|VAT RO 24708161)

RUSSIA
UCB Pharma LLC – Shturvaluaya 5 bldg 1 – 125364 Moscow (Register 1067761783341 | Tax ID 7733590603)
UCB Pharma Logistics LLC – Prensky Naberezhnye, 10, block C, 13th floor, 123112, Moscow (Register 1107746610180 | Tax ID 7701885682)

SOUTH KOREA
UCB Korea Co Ltd. – 4th Fl., FD Tower, 369 Gangnam-daero, Seocho-gu, 06621 Seoul (Register 338956)

SPAIN
UCB Pharma SA – Plaza de Manuel Gómez Moreno, s/n, Edificio Bronce, 5th floor – 28020 Madrid (Register M-455.640 | VAT ESA08338279)

SWEDEN
UCB Pharma AB (Sweden) – Olof Palmes gata 29 – 111 21 Stockholm (Register 556071-1185 | VAT SE556071118501)

SWITZERLAND
Doutors Réassurance SA – ZI de Planchy, Chemin de Croix Blanche 10 – 1630 Bulle (Register CHE-102.289.177)
UCB Farchim SA (A.G. – Ltd.) – ZI de Planchy, Chemin de Croix Blanche 10 – 1630 Bulle (Register & VAT CHE-103.818.575)
UCB Medical Devices SA – ZI de Planchy, Chemin de Croix Blanche 10 – 1630 Bulle (Register & VAT CHE-300.864.580)
UCB-Pharma AG – ZI de Planchy, Chemin de Croix Blanche 10 – 1630 Bulle (Register & VAT CHE-107.830.457)

TAIWAN
UCB Pharmaceuticals (Taiwan) Ltd – 12F.-2, No.88, Dunhua N. Rd., Songshan Dist. – 10595 Taipei (Register 54672790)

TURKEY
UCB Pharma A.S. – Palladium Tower, Barbaros Mah., Kardelen Sok. No.2, Kat.24/80 – 34746 Istanbul (Register 883001785800019 | VAT TR8830017858)

U.K.
Celltech Group Ltd – 208 Bath Road – SL1 3WE Slough, Berkshire (Register 2159282 | VAT GB 491 9583 95)
Celltech R&D Ltd – 208 Bath Road – SL1 3WE Slough, Berkshire (Register 1472269 | VAT GB 491 9583 95)
UCB (Investments) Ltd – 208 Bath Road – SL1 3WE Slough, Berkshire (Register 1106309 | VAT GB 491 958 395)
UCB Pharma Ltd – 208 Bath Road – SL1 3WE Slough, Berkshire (Register 209905 | VAT GB491 9583 95)
Zogenix Europe Limited – 208 Bath Road – SL1 3WE Slough, Berkshire
Zogenix International Limited – The Pearce Building West Street, SL6 1RL Maidenhead, Berkshire

UKRAINE
UCB Ukraine LLC – 19 Grygoriya Skovorody Str., Business – center" Podol Plaza" – 04070 Kiev (Register 38778579 | Tax ID 265613114654)

U.S.
Engage Therapeutics, Inc. – Corporation Trust Center, 1209 Orange Street – Wilmington, Delaware 19801 (Register not available yet)
Ra Pharmaceuticals, Inc. – Corporation Trust Center, 1209 Orange Street – Wilmington, Delaware 19801 (Tax ID 26-2908274)
UCB (Puerto Rico) Inc. – Corporation Trust Center, 1209 Orange Street – 19801 Wilmington, Delaware
UCB Biosciences, Inc. – Corporation Trust Center, 1209 Orange Street – 19801 Wilmington, Delaware (Tax ID 58-2415667)
UCB Holdings, Inc. – Corporation Trust Center, 1209 Orange Street – 19801 Wilmington, Delaware (Tax ID 13-3010020)
UCB Manufacturing, Inc. – Corporation Trust Center, 1209 Orange Street – 19801 Wilmington, Delaware (Tax ID 16-1502440)
UCB, Inc. – Corporation Trust Center, 1209 Orange Street – 19801 Wilmington, Delaware (Tax ID 63-078-4277)

Appendix 2 – Description of Processing and Transfers Subject to the UCB BCRs

This Appendix describes categories of Data Subjects and their Personal Data subject to the GDPR, as well as purposes for which such Transferred Personal Data are Processed by UCB BCRs Entities.

1. Categories of Data Subjects

These include Data Subjects, who are currently, had been previously or may be in the future in one of these general categories:

- **Patients and caregivers**: Patients and their relatives/family members, as well as caregivers;

- **UCB employees**: Employees, directors, and officers of UCB BCRs Entities and their relatives, as well as job applicants.

- **External workers**: All individuals, who are not UCB employees but who provide services under a contract or similar arrangement for or on behalf of UCB BCRs Entities, including contractors, independent consultants and interim workers;

- **Healthcare professionals**: All individuals who are professionally engaged in diagnosis, treatment, and delivery of healthcare, including, but not only, physicians, physician assistants, nurses, pharmacists, researchers, employees of insurance providers (both public and private), government officials;

- **Vendors**: Employees and legal representatives of external vendors/business partners providing services and/or products to UCB BCRs Entities, including, but not only, consulting firms, Contract Research Organizations (CROs), external laboratories, distributors;

- **Visitors**: Visitors to UCB facilities and events;

- **Website users**: Users, who visit websites operated by one of the UCB BCRs Entities.

2. Categories of Personal Data

The Categories of Personal Data that may be Processed or Transferred subject to these UCB BCRs include, in particular:

- **UCB BCRs Entity employee related data**: contact details (e.g., name, home and business addresses/telephone numbers/e-mail addresses, business fax number, emergency contact information), personal characteristics (e.g., gender, date of birth, birth place, marital status, family composition, nationality), national identification numbers (e.g., social security number) and electronic identifiers, educational background, professional information, such as employment history, areas of expertise, professional details (e.g., job title, position, work location), employee performance, salary, bonus, compensation and benefits, payment-related information (e.g., bank account number), work attendance data, surveys (e.g., diversity, equity and inclusion), internal employee identification number, training records, pictures, audio/visual recordings, individual profile (including, e.g., business and personal related interests), occupational health information, information related to company digital (e.g., email

usage) and other assets (e.g., company cars), systems and applications, other legally required information, background check data (e.g., related to criminal offences or convictions), information about family members (e.g., benefits data, identifiers), CCTV/image recordings;

- **Patient and caregiver related data**: personal details (e.g., name, initials, postal and email addresses, telephone number, consents given, information about healthcare providers/professionals), personal characteristics (e.g., gender, date of birth/age, education, occupation), health-related data (e.g., weight, height, medical history (including diagnosis/treatment/recovery, medication effects data), pregnancy status, images/videos of parts/areas of patient's body), individual patient identification number, ethnic origin, lifestyle, personal experience/feedback, payment-related information (including bank account number), pictures, audio/visual recordings, patients' relatives/family members related information, product diagnostics data (as it applies to patient), adverse event information, requests (e.g., information about products/programs) and other interactions (e.g., calls, emails, and related recording of the same);

- **Healthcare professional related data**: contact details (e.g., name, postal address, email address, telephone and fax numbers), internal and external identification numbers, payment-related information (including bank account number), professionals details (including job title and activities), education and qualifications, interactions with UCB BCRs Entities (e.g., field-based events, sponsored events, clinical studies, communications, online-based activities), interaction with websites and communications from UCB BCRs Entities (e.g., electronic identifiers, usage and interaction details, preferences), outlook on therapeutic concepts and approach to the products and/or therapeutic areas of UCB BCRs Entities, lifestyle (e.g., personal communication preferences), survey data related to market research and related profiling;

- **External worker data**: personal details (e.g., name, addresses, telephone and fax numbers, email addresses, ID numbers), license plate number, professional background information, payment-related information (including bank account details), personal characteristics (e.g., gender, date of birth/age, education, occupation), electronic identification information, CCTV/image recordings;

- **Vendor personnel data**: personal details (e.g., name, addresses, telephone numbers, email addresses), professional information (e.g., vendor name, job title/function, etc.);

- **Visitor data**: personal details (e.g., name, addresses, telephone numbers, email addresses), license plate number, CCTV/image recordings;

- **Website visitor related data** *(except healthcare professional/patient user-specific data covered above)*: contact details (e.g., name, addresses, telephone numbers, email addresses), login and registration related information, professional background, questions/requests submitted through the website, online identifiers, preferences/interactions with UCB BCRs Entities websites (including their content).

The types of Personal Data indicated above may be amended by the UCB BCRs Entities as needed, under the supervision and approval of the Global Privacy Team.

3. Purposes of the Processing

The BCRs apply to any Personal Data that are Processed and Transferred by UCB BCRs Entities acting as Data Exporters to UCB BCRs Entities acting as Data Importers primarily for the following purposes and any other purposes as required or expressly authorized by law:

(i) **Employment related activities**: Processing and Transfer of Personal Data for employment purposes including, recruitment; payroll and administration management; implementation of employment-related actions and obligations (including required government reporting); managing compensation, benefits and, long-term incentives; training, development and education; objectives setting and management by objectives process; resource planning, international assignment and mobility; health and safety related data processing; monitoring and evaluating employees' conducts and performances; managing talent & organizational review; analysis of workplace issues using AI techniques to gain insights and a better understanding regarding certain workforce related topics (e.g., identify and define competencies of the future, future staffing needs, identify financial loss/fraud, improve wellbeing of our employees, close the pay-gap and optimize tax benefits) and following a careful review, the application of our "Privacy by Design" approach and after informing all our employees; monitoring and managing UCB's collaborative web tools, mailboxes, and instant messaging solution, as well as other UCB information systems and all forms of electronic and digital media and services for employees' use; monitoring and managing employees' professional travels and business expenses; complying with reporting obligations required by law and internal policies and similar activities; fraud, misdemeanor and internal policy infringement prevention; monitoring and ensuring safety at the workplace and protection of UCB BCRs Entities' assets and interests; improve functionalities of internal digital assets; manage M&A transactions.

In addition to the above employment purposes, some Personal Data (such as contact details) of UCB employees, external workers and employees of external vendors may also be Processed and Transferred by UCB BCRs Entities for intra-group communication related purposes, for instance via intranet directories.

Furthermore, some Personal Data of UCB BCRs Entities' employees may also be Processed and Transferred by UCB BCRs Entities to support operational processes, for managing user's access rights to UCB IT resources (data, services and applications) and to allow collaboration between teams and individuals. The same applies to external workers and employees of external vendors.

(ii) **Research and development activities**: Processing and Transfer of Personal Data of patients and healthcare professionals (e.g., investigators) who participate in research activities initiated by UCB BCRs Entities or broader knowledge sharing opportunities, including clinical trials, epidemiological studies and similar medical research activities and other monitoring and reporting on the outcomes of various treatment paths for those purposes.

(iii) **Pharmacovigilance, reporting and product quality activities**: Processing and Transfer of Personal Data from patients and healthcare professionals in connection with drug safety and pharmacovigilance activities, in particular when handling adverse events as well as other types of product complaints, or other reporting and actions (e.g., registries maintenance, medical devices tracking, etc.) required by law.

(iv) **Activities with patients/caregivers other than (ii) and (iii)**: Processing and Transfer of Personal Data of patients/caregivers having interactions with UCB BCRs Entities, including to provide and improve assistance support programs, prescription discounts, reimbursement support programs, patient insight and engagement related activities (e.g., to provide support, train, provide/maintain/analyze communication channels to patients, in relation to UCB BCRs Entities' programs, services or products), or otherwise to provide and market (e.g., through newsletters/other materials) UCB BCRs Entities' services and products.

(v) **Handling of questions**: Processing and Transfer of Personal Data relating to Data Subjects with questions, including healthcare professionals, patients and caregivers in order to address these.

(vi) **Commercial related activities (including sales, marketing, market research/access)**: Processing and Transfer of Personal Data for customer relationship management related purposes, execution of contracts, market research, market access and any other sales and personalized marketing activities completed in the course of business activities of UCB BCRs Entities.

(vii) **External workers and vendors' personnel related activities**: Processing and Transfer of Personal Data related to external workers and personnel of external vendors in connection with the execution of the contracts signed with these external workers and vendors.

(viii) **Visitors**: Processing and Transfer of Personal Data related to visitors for access, security and emergency management purposes.

(ix) **Compliance, internal investigations and auditing**: Processing and Transfer of Personal Data for compliance, internal investigation and audit purposes. Such type of Processing may be required in certain countries for example, for transparency purposes of relationships between UCB BCRs Entities and healthcare professionals to comply with public disclosure requirements.

(x) **Legal proceedings, claims, government investigations and other legal requirements**: Processing and Transfer of Personal Data for legal proceedings and investigations by regulatory and other authorities, establishment, exercise or defense of legal claims, compliance with legal (e.g., whistleblowing) and industry standards requirements.

(xi) **Website visitor related activities** *(except healthcare professional/patient user-specific data covered above)*: Processing and Transfer of Personal Data for purposes of website management, participating/signing up for various features offered by UCB BCRs Entities' websites (e.g., newsletters, quizzes, educational/support content, etc.), responding to questions/requests submitted through websites, maintenance and monitoring of website use and related analytics and marketing activities, combining the data with other Personal Data for the above purposes.