

## Binding Corporate Rules for Data Protection and Privacy

### TABLE OF CONTENTS

1	Introduction .....	2
2	Definitions .....	3
3	Scope .....	4
	▪ Description of UCB entities bound by the BCRs	
	▪ Description of Personal Data Processing and Transfers covered by the BCRs	
	▪ Compliance by UCB BCRs entities with data protection requirements	
	▪ Compliance by UCB's employees with the BCRs	
4	Common rules applicable to Processing and intra-group Transfers.....	5
	▪ Purpose limitation	
	▪ Data quality, retention and proportionality	
	▪ Legal basis for Processing Personal Data	
	▪ Legal basis for Processing Sensitive Data	
	▪ Limited Access to Personal Data	
5	Transparency and information right .....	7
	▪ Availability of the BCRs to Data Subjects	
	▪ Information related to the Processing of Personal Data	
	▪ Rights of access, rectification, erasure and blocking of Personal Data	
6	Automated individual decisions .....	8
7	Security and confidentiality .....	8
8	Relationships with Processors that are UCB BCRs Entities .....	9
9	Restrictions on Transfers and onward Transfers to external Processors and Controllers that are not UCB BCRs Entities .....	9
10	Internal information and training .....	9
11	Audit.....	10
12	Compliance and supervision of compliance.....	10
13	Actions in case of national legislation preventing respect of BCRs .....	10
14	Internal complaint handling procedure .....	11
	▪ UCB complaints handling procedure	
	▪ Additional reporting obligations for UCB employees of UCB BCRs Entities	
	▪ Additional rights to lodge a claim before a court or data protection authority	
15	Third party beneficiary rights.....	12
16	EEA Liability .....	12
17	Cooperation with Data Protection Authorities .....	13
18	Updates of the BCRs .....	13
19	Effective Date.....	13
	Appendix 1 - UCB BCRs Entities.....	14
	Appendix 2 - Personal Data and Purposes of Processing/Transfers covered by the BCRs .	18

	<b>UCB BCRs</b>		
		Date: Nov. 30, 2015	Page 2 of 20

## 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 relating to individuals (“Data Subjects”), that may, directly or indirectly, identify these individuals (hereinafter referred as “Personal Data” and defined below).

UCB is committed to ensure the privacy of Personal Data throughout the world, and expects its employees and business partners to take the necessary measures to protect all Personal Data collected, held and Processed in the name of or on behalf of UCB. To demonstrate such commitment, UCB has included privacy as one of the group’s core values in its global Code of Conduct and designed a comprehensive Data Protection and Privacy Program in support of UCB global business processes, taking into consideration the benefits as well as the risks of innovative technologies. As two essential components of this program, UCB adopted two global privacy policies: the Global Policy on the Protection of Personal Data and the Employee Global Policy on the Protection of Personal Data (collectively the “Global Privacy Policies”).

These BCRs build upon and expand these Global Privacy Policies to ensure compliance by UCB with applicable data protection and security requirements around the world. In particular, these BCRs provide baseline standards of protection for the Processing and Transfer of Personal Data subject to the provisions of the Data Protection Directive 95/46/EC<sup>1</sup> (the “Directive 95/46/EC”) and, where applicable, the ePrivacy Directive 2002/58/EC (the “Directive 2002/58/EC”)<sup>2</sup>, or to any other relevant national data privacy laws and regulations.

The BCRs consist of the present document together with its appendices and the Global Privacy Policies. In case of contradiction between these documents, the present document of the BCRs shall prevail.

---

<sup>1</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

<sup>2</sup> 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 (also called the Cookie Directive)

	<b>UCB BCRs</b>		
		Date: Nov. 30, 2015	Page 3 of 20

## 2 DEFINITIONS

- **Binding Corporate Rules** (“BCRs”). It refers to the internal rules detailed in this document and the Global Privacy Policies to ensure data protection and privacy compliance worldwide, especially with regard to the international Transfers of Personal Data within UCB.
- **Chief Privacy Officer.** It refers to the nominated person who has the overall responsibility for developing and implementing the Data Protection and Privacy Program within UCB.
- **Competent Data Protection Authority.** It refers to any supervisory authority responsible for the protection of Personal Data.
- **Controller.** It refers to a 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 or Transfer of Personal Data.
- **Data Subjects.** It refers to any individuals whose Personal Data are Processed by UCB.
- **Local Privacy Officers.** It refers to the nominated persons in each country, who are responsible for data protection and privacy compliance in their countries, including local compliance with the BCRs.
- **Personal Data - also known as “Personal Information”.** It refers to data in any form relating to an identified or identifiable natural person, including but not limited to: name, address, telephone number, e-mail address, bank account number, image, video, patients’ key-coded information used in clinical trials, employees’ performance records, etc. An “identifiable person” is a person who can be identified, directly or indirectly, by reference to an identification number or factors.
- **Processor.** It refers to a natural or legal person, public authority, agency or any other body which Processes Personal Data for or on behalf of the Controller.
- **Processing.** It 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.
- **Sensitive Data.** It refers to a subset of Personal Data that may warrant additional protection based upon the applicable data protection and privacy local rules. Which data qualify as Sensitive Data can vary by country but such data generally comprise data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life, and data relating to offenses, criminal convictions or security measures.



- **Transfers.** It refers to the transmission of Personal Data from one country to another, or from European Economic Area<sup>3</sup> (hereinafter “EEA”) countries to locations outside the EEA. The term “transmission” includes remote access with the intent to undergo Processing.
- **UCB S.A.** It 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.

Unless otherwise specified, words or expressions, which would not be defined in the BCRs, shall have the meaning used in the Directive 95/46/EC. When applicable and insofar as possible, any reference to the Directive 95/46/EC in the BCRs will include any subsequent European data protection legislation that would replace the current Directive 95/46/EC.

Furthermore, in case of doubt, the content of the BCRs should be interpreted according to the provisions of the Directive 95/46/EC, and, where applicable, the provisions of the Directive 2002/58/EC.

### 3 SCOPE

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

The BCRs will be binding on UCB S.A. and all UCB entities (including branches) listed in Appendix 1 (collectively, the “UCB BCRs Entities”).

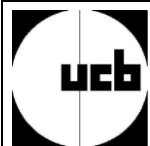
- **Data Subjects and Personal Data Processing and Transfers covered by the BCRs:**

The BCRs shall apply to all Personal Data Processing by UCB BCRs Entities and Transfers of such Personal Data between them for the purposes specified in Appendix 2, whether such Personal Data relate to:

- “Patients and caregivers”: Patients and their relatives/family members as well as caregivers
- “UCB employees”: Employees of UCB BCRs Entities (current and former employees) and their relatives/immediate family members as well as prospective employees applying for jobs to UCB BCRs Entities and directors/officers of UCB BCRs Entities
- “External workers”: Any individuals, who are not UCB employees but who provide services under a contract or similar agreement for or on behalf of UCB BCRs Entities, including contractors, independent consultants and interim workers
- “Healthcare professionals”: Any individuals who are professionally engaged in diagnosis, treatment, and delivery of healthcare, including, but not only, physicians, physician assistants, nurses, pharmacists, researchers, employees of payers, government officials

---

<sup>3</sup> EEA countries: Austria, Belgium, Bulgaria, 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, UK



- “External 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.

▪ **Compliance by UCB entities with data protection requirements:**

- When Processing or Transferring Personal Data specified in Appendix 2 throughout the world, UCB BCRs Entities will take all reasonable and necessary measures to comply with applicable data protection laws.
- To ensure a harmonized level of protection of Personal Data, even where there is no such data protection laws in a country or the local data protection laws do not meet the standards set out in the BCRs, the UCB BCRs Entities will Process Personal Data in compliance with the BCRs.
- Where applicable data protection laws in a country require a higher level of protection for Personal Data than the BCRs, such laws will prevail over these BCRs.
- The fact that UCB BCRs Entities comply with all the rules specified in the BCRs does not release them from their obligation to fulfill all the prior formalities with the relevant national authorities as required by the applicable legislation.

▪ **Compliance by UCB’s employees with the BCRs:**

The employees of UCB BCRs Entities may only Process or Transfer Personal Data specified in Appendix 2 in accordance with these BCRs and any other relevant applicable 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 disciplinary action, up to and including dismissal.

#### **4 COMMON RULES APPLICABLE TO PROCESSING AND INTRA-GROUP TRANSFERS**

For Processing and Transfers of Personal Data described in Appendix 2, UCB BCRs Entities and their employees agree to apply the following rules.

▪ **Purpose limitation:**

- Personal Data detailed in Appendix 2 will be Processed and Transferred by UCB BCRs Entities for specified, relevant and legitimate purposes, in line with the purposes defined in Appendix 2. The Personal Data Processed and Transferred shall not be further Processed in a manner incompatible with these purposes.

	<b>UCB BCRs</b>		
		Date: Nov. 30, 2015	Page 6 of 20

▪ **Data quality, retention and proportionality:**

- UCB BCRs Entities will limit the Processing of Personal Data detailed in Appendix 2 to what is necessary and proportionate in light of the pursued purpose(s).
- UCB BCRs Entities will use reasonable means to keep Personal Data accurate, complete, up-to-date and reliable for their intended use.
- UCB BCRs Entities will retain Personal Data for only as long as needed to meet the legitimate business purposes for which the Personal Data was collected and in compliance with UCB's data retention policies, unless otherwise required by applicable laws or regulations.

▪ **Legal basis for Processing Personal Data:**

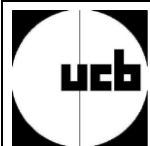
The Processing of Personal Data shall be based upon at least one of the following legal basis:

- the Data Subject's unambiguous consent; or
- 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 a legal obligation to which UCB is subject; or
- the Processing is necessary to save the vital interest of the Data 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 Controller or in a third party to whom the Personal Data is disclosed; or
- the Processing is necessary for the purposes of legitimate interests pursued by UCB except where such interests are overridden by the interests for fundamental rights and freedoms of the Data Subject.

▪ **Legal basis for Processing Sensitive Data:**

The Processing of Sensitive Data shall be based upon at least one of the following legal basis:

- the explicit consent of the Data Subject; or
- the necessity for the purposes of carrying out the obligations and specific rights of UCB in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
- 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 his Consent; or
- the Processing relates to Sensitive Data which are manifestly made public by the Data Subject; or
- the Processing of Sensitive Data is necessary for the establishment, exercise or defence of legal claims; or
- the Processing of the Sensitive Data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Sensitive Data are processed by a health



- professional 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, or
- the Processing of the Sensitive Data is required for reasons of substantial public interest laid down either by national law or decision of the supervisory authority.

▪ **Limited Access to Personal Data:**

- The Processing of Personal Data shall be limited to only those UCB BCRs Entity employees whose job role(s) and responsibility(ies) necessitate this activity.

## 5 TRANSPARENCY AND INFORMATION RIGHT

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

The BCRs will be made publically available on UCB websites to all Data Subjects whose Personal Data is subject to these BCRs.

The Data Subjects may also receive a copy of the BCRs upon request, by contacting either the relevant UCB BCRs Entities, or the Chief Privacy Officer. At a minimum, each UCB BCRs Entity shall provide a postal mail address and email address for Data Subjects to submit their request.

▪ **Information related to the Processing of Personal Data:**

So as to guarantee fair Processing in respect of Data Subjects, UCB BCRs Entities shall, having regard to the specific circumstances, offer to Data Subjects clear and conspicuous information as to the purposes of the Processing, categories of Personal Data collected, the identity of the company Processing Personal Data, how to contact UCB with any inquiries or complaints, and the choices and means offered for limiting use and disclosure of Personal Data. UCB BCRs Entities shall ensure Data Subjects are provided with any additional information required by local law.

Where UCB BCRs Entities collect Personal Data directly from Data Subjects they will provide notice in clear and conspicuous language at the time and place Data Subjects are first asked to provide their Personal Data, or as soon as practicable thereafter.

Unless applicable law provides otherwise, for Personal Data not directly collected from Data Subjects, the obligation to inform Data Subjects does not apply if the provision of such information proves impossible, or would involve a disproportionate effort, or if recording or disclosure of the Personal Data is expressly required by law.

▪ **Rights of access, rectification, erasure and blocking of Personal Data:**

UCB BCRs Entities shall ensure Data Subjects are provided with the right:

- to access, including receiving in an understandable form, any Personal Data concerning them held by UCB BCRs Entities, without constraint, at reasonable intervals and at any time the Data Subject can demonstrate well-grounded reasons, and without excessive delay or expense, in accordance with local data protections laws;
- to obtain the rectification, erasure or blocking of data due to incomplete or inaccurate Personal Data upon submission of a valid claim;
- to object, at any time on compelling legitimate grounds relating to their particular situation, to the Processing of their Personal Data, unless that Processing is required by law;
- to object, on request and free of charge, to the Processing of Personal Data relating to the Data Subject for the purposes of direct marketing.

At a minimum, each UCB BCRs Entity shall provide a postal mail and email address for Data Subjects whose Personal Data is governed by these BCRs to exercise their rights as described above.

Alternatively, Data Subjects may also contact the Chief Privacy Officer by letter or by email to [dataprivacy@ucb.com](mailto:dataprivacy@ucb.com).

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

UCB BCRs Entities may limit the Data Subjects' right to access their Personal Data in compliance with applicable local laws.

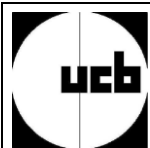
## **6 AUTOMATED INDIVIDUAL DECISIONS**

UCB BCRs Entities shall not make any decision that would significantly affect Data Subjects based solely on Processing of Personal Data by automated means with no human involvement, unless they have taken measures to protect Data Subjects' legitimate interests in accordance with applicable laws and regulations.

## **7 SECURITY AND CONFIDENTIALITY**

UCB BCRs Entities will establish and maintain 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 state of the art and will be commensurate with the risks associated with the types of Processing, the nature of the Personal Data involved, and related implementation cost. Considering their peculiar nature, Sensitive Data might require additional protective measures.





## **8 RELATIONSHIPS WITH PROCESSORS THAT ARE UCB BCRS ENTITIES**

If one UCB BCRs Entity Processes Personal Data on behalf of another UCB BCRs Entity, the UCB BCRs Entity carrying out the Processing must act only in accordance with the instructions of the UCB BCRs Entity on whose behalf the Processing is being conducted.

Furthermore, the UCB BCRs Entity carrying out the Processing on behalf of another UCB BCRs Entity must have in place technical and organizational security measures to safeguard the Personal Data that are state of the art and that are appropriate having regard to the risks associated with the types of Processing, the nature of the Personal Data involved and related implementation cost.

## **9 RESTRICTIONS ON TRANSFERS AND ONWARD TRANSFERS TO EXTERNAL PROCESSORS AND CONTROLLERS THAT ARE NOT UCB BCRS ENTITIES**

- If a UCB BCRs Entity uses an external Processor to Process Personal Data on UCB's behalf, the UCB BCRs Entity will obtain contractual commitments from such Processor to (i) only act on the instructions of the UCB BCRs Entity and (ii) have in place technical and organisational security measures to safeguard the Personal Data disclosed by the UCB BCRs Entity that are state of the art and that are appropriate having regard to the risks associated with the types of Processing, the nature of the Personal Data involved and related implementation cost.
- In addition of the above rules specific to external Processors, UCB BCRs Entities will only Transfer Personal Data to external Processors or Controllers, after ensuring an adequate level of protection for the Personal Data to be Transferred, in accordance with applicable local laws and regulations (including Articles 25 and 26 on Transfers of Personal Data of the Directive 95/46/EC when Transfers of Personal Data from UCB BCRs Entities originate from the EEA).

## **10 INTERNAL INFORMATION AND TRAINING**

In order to ensure that all employees of UCB BCRs Entities are adequately informed, UCB (globally and locally) will take all suitable steps to make these BCRs as well as related data protection procedures available to the employees.

Furthermore, all employees of UCB BCRs Entities or third parties, who have regular access to Personal Data or are involved in data collection or development of IT tools, will be provided, by UCB, globally or locally, with appropriate awareness and training materials on these BCRs and data protection rules in general.



## 11 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 Chief Privacy Officer, on applicable aspects of UCB's compliance with the BCRs on a periodic basis or whenever specifically requested by the Chief Privacy Officer and as approved by the Audit Committee. 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 Chief Privacy Officer and UCB S.A.'s Board of Directors through the Audit Committee, which will evaluate that procedures are in place to ensure that corrective action takes place as soon as reasonably practicable.

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

If requested by a Competent Data Protection Authority, the Global Internal Audit Department will also provide a copy of the results of the audit to such Competent Data Protection Authority, subject to applicable laws and respect for any confidential, privileged or commercially sensitive information provided.

## 12 COMPLIANCE AND SUPERVISION OF COMPLIANCE

UCB has appointed a Chief Privacy Officer responsible for overseeing all privacy and data protection issues, including ensuring compliance with all aspects of these BCRs. The Chief Privacy Officer reports to the VP & Chief Compliance Officer, who in turn reports to the Executive VP Global Legal Affairs.

The Chief Privacy Officer is supported by a team of Local Privacy Officers responsible for overseeing and ensuring compliance with the BCRs on a day-to-day basis at a local level. The Local Privacy Officers are to report any major privacy issues to the Chief Privacy Officer. Any other staff support may be called for from time to time and at the discretion of the Chief Privacy Officer.

## 13 ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF BCRS

If a UCB BCRs Entity discovers a conflict between local legislation and the privacy standards of these BCRs, the UCB BCRs Entity must immediately contact the Local Privacy Officer of its country or the Chief Privacy Officer.

The Local Privacy Officer or the Chief Privacy Officer will take a responsible decision on what action to take (in consultation with the Legal Department, where necessary) and will consult the relevant Competent Data Protection Authorities in case of doubt.



## 14 INTERNAL COMPLAINTS HANDLING PROCEDURE

### ▪ UCB complaints handling procedure:

Any Data Subject who believes his/her Personal Data in Appendix 2 may have been Processed in violation of these BCRs by any UCB BCRs Entity, may submit his/her questions and complaint to the Local Privacy Officer of UCB in the country where the Data Subject is located.

Any employee of UCB BCRs Entities who believes that his/her Personal Data may have been improperly Processed can either contact the local Human Resources Department or the Local Privacy Officer.

Except in the case of exceptional circumstances, the Local Privacy Officer or the local Human Resources Department (concerning UCB employees' Personal Data), will send acknowledgment of receipt of a complaint to the individual who complained within five (5) working days.

The recipient of the complaint may at his/her discretion forward the complaint to the Chief Privacy Officer /UCB Legal Department, for review, where appropriate.

The Local Privacy Officer or, if relevant, the local Human Resources Department concerning UCB employees' Personal Data, will investigate and liaise with colleagues from relevant departments as necessary to deal with the complaint. The Local Privacy Officer or local Human Resources Department shall provide a substantive response to the individual who complained as soon as reasonably practicable, but no later than one (1) month upon receiving the complaint.

If, due to the complexity of the complaint, the Local Privacy Officer or local Human Resources Department cannot provide a substantive response within one (1) month, it will notify the complainant and provide a reasonable estimate (not exceeding two (2) months) of the timeframe within which a response will be provided.

If a complainant disputes the response from the Local Privacy Officer or local Human Resources Department, he/she may appeal by notifying the Chief Privacy Officer. The Chief Privacy Officer shall review the original complaint and appeal request, and either accept the original finding or substitute a new finding. The Chief Privacy Officer will respond to the individual as soon as reasonably practicable, but no later than two (2) months of the referral of the case.

If the complaint is justified, the Chief Privacy Officer will ensure all necessary steps are taken as a result, including appropriate sanctions to employees, in accordance with local rules.

### ▪ 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, Compliance, Human Resources, or the Legal Department.



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

▪ **Additional rights to lodge a claim before a court or data protection authority:**

Irrespective of UCB's internal complaints handling procedure, the Data Subjects shall at all times be entitled to seek advice and complain to the Competent Data Protection Authority and/or to make a claim in a court of competent jurisdiction.

## 15 THIRD PARTY BENEFICIARY RIGHTS

Data Subjects whose (i) Personal Data is subject to the Directive 95/46/EC or the Swiss Federal Act on Data Protection (as amended or replaced from time to time) and (ii) Transferred to UCB BCRs Entities outside of Europe under these BCRs shall have the right to enforce the rules provided in Sections 4, 5, 6, 7, 8, 9, 13, 14, 15, 16 and 17 of these BCRs as third party beneficiaries of the BCRs for Personal Data detailed in Appendix 2 and bring the issue before the authorities/courts as specified below to seek judicial remedy arising from a breach of the rights guaranteed, including the payment of compensation.

The Data Subjects will have the rights to take their case, at their option:

- (i) to the Competent Data Protection Authority, or
- (ii) to the court of competent jurisdiction.

For the Data Subjects residing within the EEA or in Switzerland and whose Personal Data has been Transferred to UCB BCRs Entities located outside of the EEA or Switzerland, in addition to having the right to take their case to the Competent Data Protection Authority, they shall also have the right to take their case to the court of competent jurisdiction where the UCB BCRs Entity in the EEA or in Switzerland that originated the Transfer is based, or in Belgium.

The Data Subjects benefiting from the third party beneficiary rights will be informed by UCB of such rights.

## 16 EEA LIABILITY

For Personal Data originating from the EEA and Transferred outside the EEA, 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 harm an EEA resident 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 Data Protection Authorities.

In case EEA resident Data Subjects can demonstrate that they have suffered 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 was not responsible for the breach of the BCRs giving rise to those damages or that no such breach took place.

## **17 COOPERATION WITH DATA PROTECTION AUTHORITIES**

The UCB BCRs Entities shall agree to cooperate with the Competent Data Protection Authorities regarding matters related to these BCRs, to the extent such recommendations and advice do not conflict with applicable law.

The UCB BCRs Entities also undertake to respond within a reasonable timeframe to requests the Competent Data Protection Authorities may make regarding these BCRs, including audit requests, to the extent such requests are consistent with applicable law.

## **18 UPDATES OF THESE BCRs**

UCB undertakes to inform the Competent Data Protection Authorities and UCB BCRs Entities of any substantial modifications to these BCRs on an annual basis. UCB will also ensure that the Data Subjects are kept informed about the substantial changes to these BCRs.

The Chief Privacy Officer is responsible for updating the BCRs as well as the list of UCB BCRs Entities. The Chief Privacy Officer shall keep track of and record any changes to the BCRs. The Chief Privacy Officer shall make such changes available to the Competent Data Protection Authorities or the Data Subjects upon request.

No Transfer of Personal Data as specified in Appendix 2 to a UCB BCRs Entity, that is not listed in Appendix 1 and bound by the BCRs, can take place until this UCB BCRs Entity is effectively bound by the BCRs and can deliver compliance with the BCRs.

## **19 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 (it being understood that for those countries where the applicable law requires the approval by the Competent Data Protection Authority and/or the completion of certain 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). This agreement may be executed in one or more counterparts, each of which shall be deemed an original but all of which taken together shall constitute one and the same instrument.

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 Processed and/or Transferred up until termination shall remain, until these Personal Data has been erased or as long as and to the extent required by applicable laws and regulations. In the event of such change, the Chief Privacy Officer will take any required steps to update the BCRs, in accordance with the provisions of Section 18 forewith.

	<b>UCB BCRs</b>		
		Date: Nov. 30, 2015	Page 14 of 20

## **Appendix 1 – UCB BCRs Entities**

### **Austria**

UCB Pharma Gesellschaft m.b.H.

### **Australia**

UCB Australia Pty. Ltd.

### **Belgium**

UCB S.A.

UCB Pharma S.A.

UCB Biopharma SPRL

UCB Belgium S.A.

UCB Fipar S.A.

Sifar S.A.

### **Brazil**

UCB Farma Brasil Ltda

UCB Biopharma S.A.

### **Bulgaria**

UCB Bulgaria EOOD

### **Canada**

UCB Canada Inc

### **China**

UCB Trading (Shanghai) Co. Ltd.

UCB Pharma (Zhuhai) Company Limited

### **Czech Republic**

UCB s.r.o.

### **Denmark**

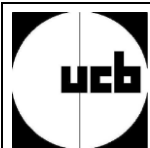
UCB Nordic AS

### **Finland**

UCB Pharma Oy

### **France**

UCB Pharma S.A.



**Germany**

UCB GmbH  
UCB Pharma GmbH  
UCB BioSciences GmbH  
Sanol GmbH  
UCB Primary Care GmbH & Co. KG

**Greece**

UCB A.E.

**Hong Kong**

UCB Pharma (Hong Kong) Ltd.

**Hungary**

UCB Hungary Ltd.

**India**

UCB India Private Limited  
Uni-Mediflex Private Limited

**Ireland**

UCB (Pharma) Ireland Ltd.  
UCB Manufacturing Ireland Ltd.

**Italy**

UCB Pharma S.p.A.

**Japan**

UCB Japan Co. Ltd.

**Luxembourg**

UCB Lux S.A.

**Mexico**

UCB de Mexico S.A. de C.V.  
Vedim S.A. de C.V.

**Norway**

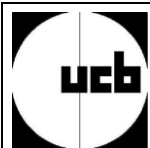
UCB Pharma A.S.

**Netherlands**

UCB Finance N.V.  
UCB Pharma B.V.

**Poland**

Vedim Sp. z.o.o.  
UCB Pharma Sp. z.o.o.



**Portugal**

UCB Pharma (Produtos Farmacêuticos) Lda

**Romania**

UCB Pharma Romania S.R.L.

**Russia**

UCB Pharma LLC

UCB Pharma Logistics LLC

**Slovakia**

UCB s.r.o.

**Spain**

Vedim Pharma S.A.

UCB Pharma S.A.

**South Korea**

Korea UCB Co. Ltd.

**Sweden**

UCB Pharma Ab

**Switzerland**

UCB Farchim SA

UCB Investissements S.A.

Doutors Réassurance S.A.

UCB-Pharma AG

UCB Medical Devices S.A.

Medeva Pharma Suisse S.A.

**Turkey**

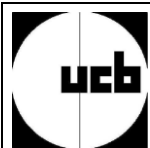
UCB Pharma A.S.

**Ukraine**

UCB Ukraine LLC

UCB Pharma GmbH Representative Office Kiev





## UCB BCRs

Date:  
Nov. 30, 2015

Page 17 of 20

### **United Kingdom**

UCB Celltech  
UCB Fipar Ltd  
Fipar UK Ltd  
UCB (Investments) Ltd.  
Celltech Group Ltd  
Celltech R&D Ltd  
UCB Ireland  
Celltech Ltd  
Darwin Discovery Ltd  
UCB Pharma Ltd  
International Medication Systems Ltd  
Schwarz Pharma Ltd

### **United States**

UCB Holdings Inc  
Fipar US Inc  
UCB Inc  
UCB Pharco Inc  
Celltech US LLC  
UCB Manufacturing Inc  
UCB Technologies Inc  
Upstate Pharma LLC  
UCB Biosciences Inc

	<b>UCB BCRs</b>		
		Date: Nov. 30, 2015	Page 18 of 20

## Appendix 2 – Personal Data and Purposes of Processing/Transfers covered by the BCRs

### **1. Categories of Personal Data Processed/Transferred between UCB BCRs Entities**

Depending on the location of the Data Subjects, the nature of their interactions with UCB BCRs Entities, and the requirements of applicable laws and regulations (in particular, data protection requirements relating to the Processing of Sensitive Data), the types of Personal Data that may be Processed by UCB BCRs Entities and Transferred between them, may include, when relevant, among other things:

- **UCB employees 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), educational background, 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), internal employee identification number, training records, pictures, audio/visual recordings, individual profile (including, e.g., business and personal related interests)
- **Patients and caregivers related data:** contact details (e.g., name, initials, postal and email addresses, telephone number), personal characteristics (e.g., gender, date of birth/age), health-related data (e.g., weight, height, medical history, pregnancy status), individual patient identification number, ethnic origin, lifestyle, personal experience, payment-related information (including bank account number), pictures, audio/visual recordings, patients' relatives/family members related information
- **Healthcare professionals 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), outlook on therapeutic concepts and approach to the products and/or therapeutic areas of UCB BCRs Entities, lifestyle (e.g., personal communication preferences)
- **External workers and vendors' related data:** contact details (e.g., name, addresses, telephone and fax numbers, email addresses), payment-related information (including bank account details)

The types of Personal Data indicated above may be amended by the Chief Privacy Officer as needed.

	<b>UCB BCRs</b>		
		Date: Nov. 30, 2015	Page 19 of 20

## **2. Purposes for Processing and intra-group Transfers**

The BCRs apply to any Personal Data that may be Processed by UCB BCRs Entities and Transferred between them as part of the global activities of the UCB group and to the extent permitted by applicable laws, for legitimate business purposes that include primarily the following purposes and any other purposes as required or expressly authorized by law:

**(i) Employment related activities:** UCB BCRs Entities may Process/Transfer UCB employees' 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; international assignment and mobility; health and safety related data processing; monitoring and evaluating employees' conducts and performances; managing talent & organizational review; 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 similar activities.


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:** UCB BCRs Entities may Process/Transfer to other UCB BCRs Entities Personal Data from patients and healthcare professionals (e.g., investigators) who participate in research activities initiated by UCB BCRs Entities, including clinical trials, epidemiological studies and similar medical research activities.

**(iii) Pharmacovigilance and product quality activities:** UCB BCRs Entities may Process/Transfer to other UCB BCRs Entities 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, in order for UCB BCRs Entities to comply with relevant legal requirements.

**(iv) Activities with patients/caregivers other than (ii) and (iii):** UCB BCRs Entities may Process/Transfer to other UCB BCRs Entities Personal Data from patients/caregivers having interactions with UCB, including patients who may be involved in patients assistance support programs, prescription discounts, reimbursement support programs, patient insight related activities.

	<b>UCB BCRs</b>		
		Date: Nov. 30, 2015	Page 20 of 20

**(v) Handling of medical questions:** UCB BCRs Entities may Process/Transfer to other UCB BCRs Entities Personal Data relating to persons contacting them with medical questions, including healthcare professionals, patients and caregivers.

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

**(vii) External workers and vendors related activities:** UCB BCRs Entities may Process/Transfer to other UCB BCRs Entities Personal Data relating to external workers and employees of external vendors in connection with the execution of the contracts signed with these external workers and vendors.

**(viii) Compliance, internal investigations and auditing:** UCB BCRs Entities may Process/Transfer Personal Data to other UCB BCRs Entities 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.

**(ix) Legal proceedings and government investigations:** UCB BCRs Entities may Process and Transfer Personal Data to other UCB BCRs Entities in connection with legal proceedings and investigations by regulatory bodies.

### **3. Description of intra-group Transfers between UCB BCRs Entities**

To effectively conduct their global activities, the Processing of Personal Data by UCB BCRs Entities, in connection with purposes identified in the BCRs, may involve international transfers of Personal Data from their employees or any other types of Data Subjects mentioned above, from any UCB BCRs Entity to any other UCB BCRs Entity, including, to a large extent but not only, from EEA countries and, in particular, Belgium, where the UCB group has several central servers located.