Binding corporate rules as controller

Our BCRs Controller is applicable only to the Concentrix Affiliate under Concentrix SAS, the latter acting as the European Lead Entity

The Affiliates to which the BCRs apply are listed in Appendix 01 of the BCRs.

Content

1. Introduction

Reminder: Following the Webhelp & Concentrix transaction of September 2023, the commercial name of the group is now Concentrix. However, please note that the scope of the present BCR has not been modified. The BCRs are only applicable to the Affiliates under Concentrix SAS acting as European Lead Entity, Affiliates that are bound by the BCR (Controller and/or Processor) are listed in Appendix 01 and shall be referred as BCR Member.

At Concentrix Group, we believe that protecting Personal Data is not only a matter of security or compliance with a particular legal framework, but is a matter of individual and organisational commitment. Disclosing and sharing Concentrix standardsthrough , the Binding Corporate Rules for Processors (hereinafter the "BCR-P") and the present Binding Corporate Rules for Controllers (hereinafter the "BCR-C") is of the utmost importance regarding the Data Subjects' legitimate expectations about how their Personal Data is Processed.

In the course of its activities, BCRs Members process both internal and Client Personal Data. In this respect, BCRs Membersprotect the Personal Data it processes on its own behalf by the implementation of appropriate technical, physical and administrative measures and controls, comprised in the present BCR-C. Such controls shall ensure that the whole organisation is Processing Personal Data in a consistent manner, disregarding the nature and/or place of Processing.

This approach is particularly important due to the diversity of activities Concentrix covers on behalf of its Clients.

As a consequence of the above and taking into consideration the requirements introduced by the European Regulation 2016/679 adopted on 27 April 2016 (hereinafter, the "**EU Regulation"** or **"GDPR"**) and standards, regulations and laws applicable in the field of data protection, where they do not contrevene with the EU Regulation, BCR Members will Process Personal Data in accordance with the following principles:

- **Lawfulness** – Personal Data shall be collected and Processed with the Data Subject having given consent to the Processing or when Processing is legitimate or necessary in accordance with Applicable Data Protection Legislation;
- **Fairness** – Personal Data Processing shall take into account the specific circumstances and context in which such Personal Data is Processed;
- **Transparency** – Information and communication relating to the Processing of Personal Data shall be easily accessible, easy to understand, clear and in plain and simple language;
- **Purpose limitation** – Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes;
- **Data minimisation** – Collected Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed;
- **Accuracy** – Personal Data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data

that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without undue delay;

- **Storage limitation** – Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed or any other lawful retention;
- **Integrity and confidentiality** – Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical, physical and administrative measures.

Through this BCR-C Concentrix intends to share and specify the detail and the principles applicable to all BCR Members and provide certain group-wide standards allowing the implementation of the BCR-C. Furthermore, Concentrix may make available specific, local or sectorial policies. Should there be a contradiction between this BCR-C and such specific, local or sectorial policies, the terms of the BCR-C shall prevail, unless the contradictory provisions of such specific, local or sectorial policies are more protective of the Data Subject rights and freedom.

As the BCR-C aims at ensuring an adequate and consistent approach throughout the entire Concentrix organisation regarding Personal Data Processing, exceptions which could result from applicable legislations are not reflected in this BCR-C. However, this BCR-C comprises a notification mechanism in section 12.3 where national legislation prevents a BCR Member from complying with the BCR-Cand where specific rules adding to the EU Regulation are provided by EU Member States. As a consequence, local legislation shall be considered as an enforceable exception to this BCR-Cand will be recorded accordingly, following appropriate notification. As specified in section 12.3, where this national legislation imposes a higher level of protection for Personal Data, this national legislation will take precedence over the BCR-C.

2. Scope

2.1 Material scope

This BCR-C is applicable whenever a a BCR Member Processes Personal Data as Data Controller and as a Data Processor for Processing carried out within the Concentrix organization, on behalf of a BCR Member acting as Data Controller.

Due to the diverse range of activities Concentrix covers, Concentrix may have to process various and constantly evolving categories of Personal Data, such as:

Data relating to personal life (e.g. recruitment management, camera recording system, client and prospect lead management) ;

- Economic and financial data (e.g. payroll management, client and prospect lead management,) ;
- Identification data (e.g. suppliers management, non-commercial communication, survey and form, client and prospect lead management) ;
- Technical data (e.g. IT and telephony management, badge management, employee record management) ; or

- Transactional data (e.g. corporate and legal entities management).

The material scope is more precisely detailed in **Appendix 11-A** which provides a detailed table on the Purpose of Processing and the related categories of Data Subjects and Personal data covered by the present BCR-C. **Appendix 01** provides information on the third countries and BCR Members to which Personal Data is transferred.

BCR-C shall apply to all Data Subjects whose Personal Data are transferred within the scope of the BCR-C from a BCR Member under the scope of application of the GDPR. Therefore, the BCR Member acknolewdges that the scope of the BCR-C may, in particular, not be limited to “EEA citizens or EEA residents”.

In addition, this BCR-C applies to the Processing of Personal Data by a BCR Member acting as Data Controller or as Data Processor on behalf of another BCR Member acting as Data Controller, irrespective of the category and nature of such Personal Data.

Furthermore, each BCR Member is also the Data Controller of the Personal Data of its employees as their employer. When Processing Personal Data of ts employees, BCR Members will comply with this BCR-C and will Process Personal Data as described in the Employee Privacy Policy.

2.2 Geographical scope

Concentrix wants to deploy as much as possible a consistent approach within the organization where Personal Data are being Processed. Consequently, all BCR Members, whatever their location or legal jurisdiction, are subject to this BCR-C. Therefore, the present BCR-C shall at least apply to all Personal Data transferred to BCR Members outside the EEA, and onward transfers to other BCR Members outside the EEA. Please be reminded Concentrix entities bound by the present BCR-C (i.e., BCR Members) are listed in Appendix 01.

As a principle, no Transfer of Personal Data shall be carried out by any Concentrix entities unless and until it is bound by this BCR-C to a Concentrix entities not bound by this BCR-C. Any such Transfer cannot be carried out unless this Concentrix affiliate has provided sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing and obligations attached to such Processing will meet the requirements of this BCR-C and ensure the protection of the rights of the Data Subjects.

The BCR Member bound by the BCR-C and the Concentrix entities not bound will enter into a written agreement to guarantee this.

3. Binding nature

3.1 Upon employees of Concentrix

Each BCR Member’s employee, as a Data Subject, shall benefit from the provisions of this BCR-C. As protecting Personal Data is a matter of individual and organisational commitment, each employee must also comply with the requirements specified under this BCR-C.

As such, the BCR-C falls within the set of policies Concentrix employees are required to comply with as part of their employment contract. Failure to comply with the principles and rules of this BCR-C may lead to disciplinary action that could result in the termination of the employment and, in certain circumstances, to criminal charges.

3.2 Upon BCR Members of Concentrix group

As a group, Concentrix wants to ensure that all BCR Members belonging thereto are bound in the same or a similar manner to the principles and obligations specified under this BCR-C and will comply with the requirements specified herein.

For this reason, this BCR-C is binding upon all the BCR Member by signing an Intragroup Data Transfer Agreement comprising this BCR-C as an appendix.

The list of Concentrix entities bound by this BCR-C is set out in Appendix 1 to this BCR-C. Concentrix SAS as Lead European Entity, with the assistance of the DPO, commits to keep this list up-to-date and available and to communicate it on request to the relevant parties as determined from time to time.

3.3 Towards Concentrixes' Data Processors

Where a BCR Member engages a Data Processor (be it a BCR Member, an affiliate of the Concentrix group not yet bound by the BCR or a third party provider) for carrying out specific Processing activities, such Data Processor shall provide sufficient guarantees to implement appropriate technical and organisational measures in a manner that the Processing will meet the requirements of this BCR-C.

Therefore, any Processing activity undertaken by BCR Member's Data Processors shall be governed by a written contract or other binding legal act, and shall set out all elements of article 28 GDPR as reminded below and in particular the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of BCR Member acting as Data Controller.

In addition, this contract or other binding legal act with a Data Processor shall set out the following provisions:

1. The Data Processor shall process the Personal Data only on documented instructions from the Data Controller, including with regards to Personal Data Transfers, uless required to do so by Union or Member State law to which the Data Processor is subject (in such case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such informationon important grounds of public interest).
2. The Data Processor shall keep the Personal Data confidential especially by ensuring that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3. The Data Processor shall take appropriate technical, physical and organizational security measures to ensure an appropriate level of security to protect the Personal Data.
4. The Data Processor shall not permit Sub-Processor to Process Personal Data in connection with its obligation to a BCR Member without the prior written authorization of the BCR Member and shall ensure this Sub-Processor undertakes to comply with the same obligations as provided in the binding act executed between the Data Processor and the BCR Member by way of a contract or other legal act under Union or Member State law. Where the Sub-Processor fails to fulfil its data protection obligations, the initial Data Processor shall remain fully liable to the BCR Member for the performance of that other Data Processor's obligations.
5. The Data Processor shall provide all necessary support to the BCR Member with regards to the handling of requests from Data Subjects relating to their rights.
6. The Data Processor shall provide all reasonable assistance to the BCR Member to:
    - Ensure a level of security of the Processing appropriate to the risk,
    - Without undue delay, inform the BCR Member of any actual or suspected security breach involving Personal Data and support the BCR Member in the notification to the relevant Supervisory Authority and communication to affected Data Subjects as the case may be.
    - Conduct data protection impact assessment (DPIA) and, where relevant obtain prior consultation with the Supervisory Authority where the DPIA result in a high risk in the absence of measures to mitigate the risk.
7. The Data Processor shall comply with the BCR Member's instructions regarding the deletion or return of the personal data at the termination of the contract or other legal binding act, and delete existing copies unless Union or Member State law requires storage of the Personal Data.
8. The Data Processor shall make available to the BCR Member all information necessary to demonstrate its compliance and contribute to audits and inspections by a BCR Member or other relevant authority or auditor mandated by the BCR Member.
9. The Data Processor shall immediately inform the BCR Member if, in its opinion, an instruction infringes this BCR-C or relevant Applicable Data Protection Legislation.

4. Principles for processing personal data

The Applicable Data Protection Legislation defines a set of principles to be observed when Processing Personal Data. Concentrix undertakes to comply with these principles acting as Data Controller or Data Processor on behalf of a BCR Member acting as Data Controller.

4.1 Defining a legal basis for Processing (Transparency, fairness and lawfulness)

When Personal Data is being Processed, it is required that such Processing relies upon an appropriate legal basis as those provided for in article 6 GDPR, such legal basis being the foundation that allows for lawful Processing.BCR Members acknowledge that one of the following legal basis may be applicable fo the Processing of Personal:

- Data Subjects' consent;
- Performance of a contract to which the Data Subject is party or to enter into such contract
- Legal obligation set out under the Union or Member State lawto which the Data Controller is subject
- Vital interest of the Data Subjects or another individual
- Performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
- Legitimate interest of the Data Controller or of a third party (provided such interest does not override the rights and freedom of the Data Subjects).
- Or any other

In this respect, BCR Members undertake to lawfully Process Personal Data only where it has a valid legal basis to do so pursuant to the requirements of the Applicable Data Protection Legislation.

For instance, the Processing of Concentrix employees' Personal Data is necessary to manage leave requests (e.g. holidays). Thus, the legal basis for such processing operation is the necessity to execute the employment contract Concentrix and its employees have entered into.

In addition, and in line with Article 5 below BCR Members undertake to ensure that:

- Special Categories of Personal Data may only be processed in line with one the exemptions envisaged by Article 9(2) GDPR apply,, and
- Processing of Personal data relating to criminal convictions and offences shall be prohibited, unless the same exemptions as the ones envisaged by Article 10 GDPR apply.

4.2 Defining a purpose (Purpose limitation)

Unless specifically authorised by Applicable Data Protection Legislation, BCR Members shall ensure that it has ascertained a lawful, fair, explicit and legitimate purpose prior to any collection or Processing of Personal Data.

BCR Members undertake to ensure that the purposes it defines do not breach the Applicable Data Protection Legislation and appear to be legitimate while ensuring Personal Data is not further Processed in a manner that is incompatible with those purposes.

For instance, planning the necessary work force to deliver its services and consequently managing Concentrix employees' schedules is one of the purposes defined for the collection of Employees' personal data regarding their request for leave.

4.3 Minimizing Personal Data collection(Data minimization)

BCR Members commit to collect and process Personal Data which is strictly adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

Personal Data shall not be collected widely in the perspective of a further undefined purpose.

For instance, Personal Data collected for managing request for leave is limited to the nature of the leave (e.g. holidays, maternity leave etc.) and other relevant information (e.g. duration of the leave), but it does not include any Personal Data which is not strictly necessary (such as with whom the employee is going on holidays, the destination of the employee or any health data for sick leaves).

4.4 Holding a record

Whether acting as a Data Controller or Data Processor, BCR Members shall maintain a record of all categories of Personal Data Processing activities under its responsibility in order to demonstrate compliance with the BCR-C.

Where acting as Data Controller, the Record of Processing Activities should at least mention the following information in line with Article 30.1 of the GDPR:

- The name and contact details of the Concentrix entity, the potential joint controller and the Data Protection Officer;
- The purposes of the Processing;
- The description of the categories of Data Subjects and of Personal Data;
- The categories of recipients of the Personal Data;
- The potential transfers of Personal Data to a third country or an international organisation;
- The Data storage duration;
- A general description of the technical and organisational security measures to ensure a level of security appropriate to the risk of the Processing.

For instance, the Processing operation of managing employees' requests for leave is included in the Record of Processing Activities related to employee administrative management which contains the above listed information.

Where acting as Data Processor, the Record of Processing Activities should at least mention the following information in line with Article 30.2 of the GDPR:

- The name and contact details of the the Processor(s) and of each Controller on behalf of which the processor is acting, and, where applicable, of the Contrllers's or 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 and, in the appropriate safeguards or exemption applicable in line with Article 49 of the GDPR.

4.5 Accuracy of the Personal Data (Data Accuracy)

BCR Members shall implement adequate measures and controls to ensure that the Personal Data it collects and processes remains accurate and, where necessary, kept up to date. To this end, BCR Members undertake to implement any required actions to take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is Processed, is erased or rectified.

For instance, Employees have a duty to inform their HR department of any update in their personal situation (e.g. address modification). BCR Members will then ensure the Personal Data will be updated accordingly in the Employees' record.

4.6 Defining a data retention period (Limited storage period)

BCR Members will not keep the Personal Data for a longer period than is strictly necessary having regard to the purpose for which such Personal Data is collected. In this respect, BCR Members commit to determine a data retention period before implementing each Processing.

To ensure compliance with this requirement, BCR Members shall implement a data retention procedure and specify guidelines to be applied with respect to a given Processing activity.

For instance, Personal Data collected for managing leave request are kept as long as necessary to manage the schedules, perform action relating to payroll (e.g. unpaid leave) and to comply with applicable local statute of limitation and accounting obligations.

4.7 Implementing security measures (integrity and confidentiality)

BCR Members have implemented appropriate technical, physical and administrative measures and controls to ensure that Personal Data is not unlawfully accessed and/or Processed. Such technical, physical and administrative measures shall ensure a level of security appropriate to the risk, including, but not limited to, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by any BCR Member and any Data Processor.

In addition, BCR Members ensure that its subcontractors / Processors comply with the technical and organisational security measures implemented at Concentrix by entering into written agreements with them comprising the requirements set out in article 28.3 GDPR (see also Article 3.3 of the BCR-C above).

For instance, BCR Members have elaborated and implemented an Information Security Policy (Appendix 10 to this BCR-C). Locally, BCR Members may have also implemented more specific security policies. When entering into an agreement with subcontractors / Processors, BCR Members reserve themselves the right to assess the level of security provided by the contracting party to the Processing of Personal Data.

4.8 Data Protection Impact Assessment

The Data Protection Impact Assessment (DPIA) is a risk-based process introduced by the General Data Protection Regulation that enables the Data Controller to describe the Personal Data Processing, to prove its necessity and proportionality and to help manage the risks to the rights and freedoms of natural persons resulting from the Processing of Personal Data by assessing them and determining the measures to address them. BCR Members are committed to conduct DPIAs in accordance with **Appendix 09 Procedure for Data Protection Impact Assessment**.

Where a type of Processing, involving in particular the use of new technologies, is likely to result in a high Risk to the rights and freedoms of Data Subjects, BCR Members shall, taking into account the nature, scope, context and purposes of the processing and prior to the processing, carry out a DPIA. This requirement shall also apply to existing Processing operations where a modification of the processing operation is expected and where such modification may result in a high Risk to the rights and freedoms of Data Subjects.

The processing would require a Data Protection Impact Assessment if two or more of the following is correct:

- The Data processing includes systematic evaluation or scoring of personal aspects relating to natural persons, including profiling and predicting;
- The Data processing is based on automated processing that significantly affects the natural person;
- The Data processing is done on sensitive Data or on Data of highly personal nature;
- The Data is processed on a large scale;
- The processing combines or matches two or more Data processing operations;
- The Data processing includes a systematic monitoring of a publicly accessible area;
- The processing is made on vulnerable persons' or kids' Data;
- The Data processing includes innovative use or application or technological or organisational solutions;
- The Data processing is made for the purposes than those for which the Data were collected;
- The Data processing prevents the Data subjects from exercising their rights or using a service or contract.

In addition, BCR Members shall carry out a DPIA for Processing operations that require a DPIA pursuant to a decision of the relevant EEA Supervisory Authority's list of data processing operations that require a DPIA.

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 and where a DPIA reveals high residual Risks, BCR Member will seek prior consultation of the EEA Supervisory Authority before carrying out this Processing.

For instance, managing employees' leave request is not a processing considered to present a high risks to the rights and freedoms of Data Subjects. Although, whenever a BCR Member identifies a processing meeting two or more of the

above-listed criteria, a DPIA is conducted under the supervision of the DPO in accordance with the procedure further described in Appendix 9.

4.9 Subprocessing and Transfers outside the Concentrix Group

BCR Members undertake not to Transfer any Personal Data to Data Controllers and/or Data Processors which are not a BCR Member unless such Data Controllers and/or Data Processors provide sufficient guarantees and have implemented appropriate technical and organisational measures, such as the ones provided in the BCR-C, in such a manner that the Processing will meet the requirements of this BCR-C.

In this respect, BCR Members have implemented appropriate technical, physical and administrative measures to ensure and control that Personal Data is not unlawfully accessed and/or Processed.

Any BCR Member is required to enter into a written contract or other binding legal act with any Data Controllers or Data Processors outside the Concentrix Group (or not bound by the BCR-C) if they are Processing Personal Data. The above-mentioned contract or other binding legal act, shall set out the elements mentioned in Article 3.3 . Such contract may include this BCR-C.

Thus, if a BCR Member, acting as Data Controller or Data Processor on behalf of another BCR Member, uses the services of a subcontractor which is established outside the EEA and needs for the Purpose of the services being performed to share its employees' Personal Data (only to the extent necessary for the operations), BCR Member shall assess, prior to the Transfer, that the subcontractor is able to meet the requirements of the BCR-C and secure the Transfer by the appropriate binding legal act.

4.10 Implementing Personal Data Breach notification measures

Where a Personal Data Breach occurs, BCR Members shall comply with the applicable Data Breach procedure adopted by Concentrix.

In any case, BCR Membersshall without undue delay, and where feasible, not later than 72 hours after having become aware of it, notify the Personal Data Breach to (1) Concentrix SAS (as the Liable BCR Member) and the other relevant Local Privacy Leaders when such BCR Memberis acting as a Data Controller , as well as to the BCR Member acting as a Controller when a BCR Member acting as a processor becomes aware of a Personal Data Breach (2) the competent EEA Supervisory Authority, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The above-mentioned notification shall cover at least the following information:

- Nature of the Personal Data Breach and scope of the Personal Data Breach, including when possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

- Name and contact detail of the (Group) Data Protection Officer ("**DPO**") or other contact point where more information can be obtained
- Describe the consequences likely to result from the Personal Data Breach;
- Describe the measures taken or proposed to be taken by the Data Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Any BCR Member, when Processing Personal Data on its own behalf as a Controller, and when Processing Personal Data on behalf of another BCR Member acting as a Controller , may also need to communicate to the Data Subjects about the Personal Data Breach where such Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons in line with Article 34 of the GDPR. In such circumstances, the communication shall take place without undue delay, and shall cover the above-mentioned elements as the one which would be communicated to the competent EEA Supervisory Authority.

BCR Members shall document any Personal Data Breach and the above mentioned information. Upon request, BCR Members shall make this documentation available to the competent EEA Supervisory Authority.

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, BCR Members will proceed in accordance with the Personal Breach procedure described in **Appendix 08 Procedure for Personal Data Breach Notification**.

5. Processing sensitive data

BCR Members undertake to comply with the provisions of Article 4 – Principles for Processing Personal Data and acknowledges that Sensitive Personal Data requires the implementation of specific protection as such Personal Data could create significant risks in relation to fundamental rights and freedoms of Data Subjects.

BCR Members undertake to process Sensitive Personal Data in accordance with Applicable Data Protection Legislation and where applicable any other sectorial applicable framework adopted by EEA Supervisory Authorities.

Such Processing shall be limited and specific, in particular in relation to Concentrix employees.

Where it intends to process Sensitive Personal Data on its own behalf, BCR Members will ensure that:

- The Processing is necessary and lawful; or
- The Processing is carried out with appropriate safeguards and controls; or
- When necessary, the Data Subject has given explicit consent to the Processing of those Sensitive Personal Data for one or more specified purposes. Such consent shall not be considered as necessary when (1) the Data Subject is not in a position to give his/her consent and the Processing is necessary to protect the vital interests of the Data Subject or of another person; (2) the Data Subject itself has already manifestly rendered the affected Sensitive Personal Data part of the public domain; (3) When applicable, the Processing is explicitly permitted by Applicable Data

Protection Legislation or any national law (e.g. registration/protection of minorities); or

- When necessary, the Processing is essential for the purpose of establishing, exercising or defending legal claims, provided that there are no grounds for assuming that the Data Subject has an overriding legitimate interest in ensuring that such data is not Processed.

6. Transfer of Personal Data to third countries and restriction on onward Transfer to non BCR Members

6.1 Transfers and onward Tansfers of Personal Data

In the course of their business, BCRs Members may Transfer Personal Data to other entities of Concentrix group (which are BCR Members or not) or to third parties. Such entities of Concentrix and/or third parties may be located outside the European Economic Area (hereinafter "**EEA**"). In such a case, Transfers of Personal Data are deemed to take place.

Where Personal Data is Transferred, Concentrix will implement specific guarantees in order to ensure that the Personal Data transferred benefit from an adequate level of protection as further detailed below:

- Transfers of Personal Data from a BCR Member, acting as Data Controller to another BCR Member located outside of the EEA and acting either as Data Controller or as Data Processor will be supported by the provisions of this BCR-C; or
- Transfers of Personal Data from a BCR Member acting as Data Controller to either an entity of Concentrix group (which is not a BCR Member) or to third parties which are located outside of the EEA (more, specifically in a non-EEA country that has been granted an adequacy decision by the EU Commission) and that are acting as Data Processor will be supported by a written agreement including the applicable standard contractual clauses adopted by the competent EEA Supervisory Authority and/or the EU Commission, -such as the EU Commission SCCs on Transfers (914/2021), Module 2 Controller to Processor; or;
- Transfers of Personal Data from a BCR Member acting as Data Controller to either an entity of Concentrix (which is not a BCR Member) or to third parties located outside of the EEA, (more, specifically in a non-EEA country that has been granted an adequacy decision by the EU Commission) and that are acting as Data Controller will be supported by a written agreement including the applicable standard contractual clauses adopted by the competent EEA Supervisory Authority and/or the EU Commission such as the EU Commission SCCs on Transfers (914/2021), Module 1 Controller to Controller).
- In the absence of an adequacy decision or appropriate safeguards as descirived above, Transfers may exceptionally take place if a derogation applies in line with Article 49 GDPR and shall, where relevant be occasional and not repetitive.

In any event, BCR Members commits not to transfer Personal Data to third parties which are not part of the Concentrix group (or to a Concentrix entity which is not a BCR Member) without ensuring first that an adequate level of protection in line with the one provided by the GDPR will be granted to the Personal Data transferred so as to ensure that the level of protection of Data Subjects guaranted under the GDPR is not undermined.

More specifically, BCR Members agree that Personal data that have been transferred under the BCR-C between two BCR Members may only be onward transferred outside the EEA to Data Pocessors and Controllers not bound by the BCR-C provided that the requirements on Transfers set out in Article 44 to 46 of the GDPR and reflected herein are complied with.

6.2 Obligation of the Data Importer in case of government access request

Without prejudice to the obligation of the BCR Member acting as Data Importer to inform the Data Exporter of its inability to comply with the commitments contained in the BCR-C (Article 12.3 below), BCR Member acting as Data Importer will promptly notify the Data Exporter and, where possible, the Data Subject (if necessary with the help of the Data Exporter) if it:

- Receives a legally binding request by a public authority under the laws of the country of destination, or of an another third country, for disclosure of Personal Data transferred pursuant to the BCR-C. Such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided;
- Becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the BCR-C in accordance with the laws of the country of destination. Such notification will include all information available to the Data Importer.

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

The Data Importer will provide the BCR Member acting as Data Exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly.

The Data Importer will preserve the above mentioned information for as long as the Personal Data are subject to the safeguards provided by the BCR-C, and shall make it available to the Competent Supervisory Authority upon request.

The Data Importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of

the country of destination, applicable obligations under international law, and principles of international comity.

The Data Importer will, under the same conditions, pursue possibilities of appeal.

When challenging a request, the Data Importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

The Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It will also make it available to the Competent Supervisory Authority upon request.

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

In any case, Transfers of Personal Data by a BCR Member to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society (see Article 12.3 of the BCR-C in this regards).

7. Rights of Data Subject

7.1 Third Party beneficiary Rights

Whenever a BCR Member Processing Personal Data as Data Controller or as Processor Processing Personal Data on its behalf, **Data Subjects are entitled to enforce this BCR-C as third-party beneficiaries.**

Data Subjects must at least be able to enforce the following elements:

- Legal basis for processing (Article 4.1);
- Purpose limitation of the Processing (Article 4.2);
- Data 16inimization (Article 4.3);
- Limitation of the storage periods (Article 4.6);
- Data accuracy (Article 4.5);
- Security of Personal Data, especially
    - Data protection by design and by default and measures to ensure data security (Articles 12 and 4.7);
    - Personal Data Breach notification where the Personal Data breach is likely to result in a high risk to their rights and freedoms (Article 4.10)
- Specific rules when processing of special categories of Personal Data and Personal Data related to criminal convictions and offences (Article 5);
- Transparency and easy access to this BCR-C; (Article 12.1);
- Onwards transfers (Article 4.9);
- Rights of access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction to each recipient to whom the personal data have been disclosed, objection to processing, right to data portability,

right not to be subject to decisions based solely on automated processing, including profiling; (Article 7.4 and 7.5)
- National legislation preventing respect of BCRs (Article 12.3)) and in case of government access requests (Article 6.2);
- Right to complain through the internal complaint mechanism of the companies (Article 8 of the BCRs and Appendix 5 – Article 3.1);
- Cooperation duties with EEA Supervisory Authority (Article 12.4);
- Right to lodge a complaint with the competent EEA Supervisory Authority (choice before the supervisory authority in the Member State of his habitual residence, place of work or place of the alleged infringement) and before the competent court of the EU Member State (choice for the Data Subject to act before the courts where the controller or processor has an establishment or where the Data Subject has his or her habitual residence) (Article 8);
- Duty to inform the Data Subjects about any update of the BCR-C and of the list of BCR Members that are bound by the present BCR-C (Article 13);
- The present Third-party beneficiary rights (Article 7);
- Right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCR-C (Article 7 and 8 of the BCRs, and Appendix 5 – Article 3.4.2);

Thus, BCR Members acknowledge that Data Subjects are entitled to seek judicial remedies and/or remedies before a data protection authority under the conditions defined below, for any non- compliance with one of the enforceable elements of the BCR-C as enumerated above and to receive compensation for any damages resulting from the violation of the BCR-C by any BCR Member.

A BCR Member accepts that Data Subjects may be represented by a not-for-profit body, organisation or association to lodge the complaint on his or her behalf, to exercise the rights enumerated above. Such body, organization or association shall have been properly constituted in accordance with the law of a Member State, have statutory objectives which are in the public interest, and be active in the field of the protection of Data Subjects' rights and freedoms with regard to the protection of their Personal Data.

For the sake of clarity, it is specified that the third party beneficiary rights above described do not extend to those elements of the BCR-C pertaining to internal mechanisms implemented within entities, such as details of training, audit programme, compliance network, and mechanism for updating the BCR-C.

Please note that withouth prejudice to the present Article 7, Concentrix encourages Data Subjects to use the internal complaint mechanism described in Article 8 of the BCRs-C provided below.

7.2 Right to lodge a complaint and obtain judicial remedy, redress and compensation where a BCR Member within the EEA does not comply with the BCR-C

Where a BCR Member within the EEA does not comply with one of the enforceable elements of the BCR-C as enumerated in the previous section 7.1 above, Concentrix acknowledges that the BCR Member within the EEA responsible for the non-compliance, shall bear responsibility and shall take the necessary actions in order to remedy its acts.

.

Concentrix also acknowledges that the Data Subject shall be entitled to:

- lodge a complaint with an EEA Supervisory Authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement; and/or;
- an effective judicial remedy where he or she claims that this BCR-C has been infringed by a BCR Member as Data Controller or by a BCR Member as a Processor Processing Personal Data on its behalf. Concentrix acknowledges that such claim can be brought either before the competent court of the Member State where the BCR Member responsible for the non-compliance is established or before the court where the Data Subject has his or her habitual place of residence.

7.3 Right to lodge a complaint and obtain judicial remedy, redress and compensation where a BCR Member outside of the EEA does not comply with the BCR-C

Where a BCR Member outside of the EEA does not comply with one of the enforceable elements of the BCR-C as enumerated above, Concentrix SAS as European Lead Entity (1) accepts to be the "Liable BCR Member" and as such endorses responsibility for any material and non-material damages resulting from the non-compliance with the BCR-C, including payment of compensation when granted by the competent court, and (2) agrees to take the necessary actions in order to remedy the acts of such other BCR Member outside the EEA.

.

In such circumstances, Concentrix SAS also acknowledges that any Data Subject who considers that the BCR Member located outside the EEA (acting as Data Controller or Data Processor) has breached one of the enforceable elements enumerated in Section 7.1, shall be entitled to:

- lodge a claim with a data protection authority where he/she has his/her place of residence, place of work or where the BCR Member with delegated responsibility is established. And/or;
- an effective judicial remedy as if the violation had been caused by Concentrix SAS instead of the non-EEA located BCR Member, before the courts or judicial authorities where Concentrix SAS is based, or where the Data Subjects has his/her place of residence or place of work

Where Data Subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the

breach of the BCR-C, Concentrix SAS will be responsible for demonstrating that such BCR Member outside the EEA was not responsible for the breach of the BCR-C giving rise to those damages, or that no such breach took place. In the event Concentrix SAS can demonstrate that the other BCR Member located outside the EEA was not responsible for the act, then it can also discharge itself from any responsibility.

7.4 Data Subjects Rights

Data Subjects are entitled to benefit from the following rights:

- Have access to the Personal Data relating to him/her and Processed by a BCR Member;
- Request the rectification or deletion of any inaccurate or incomplete Personal Data relating to him/her, and of any Personal Data with respect to which the purpose of Processing is no longer legal or appropriate;
- Request that the Personal Data Processing relating to him/her be limited;
- Object to the Processing of their Personal Data by a BCR Member where such Processing is necessary for the purposes of the legitimate interests pursued by the BCR Member acting as a Data Controller or by a third party, for legitimate interests purposes, including profiling at any time, on grounds relating to their personal individual situation, unless the interets pursued by the BCR Member override the interests rights and freedoms of the Data Subjects;
- Object to the Processing of their Personal Data for marketing purposes, inluding profiling; and
- Receive their Personal Data in a structured, commonly used, machine-readable format and interoperable when the Processing is carried out by automated means

Where a BCR Member is acting as Data Controller, it will handle such request without undue delay and in accordance with the complaint handling procedure specified under Section 8 below.

The BCR Member acting as Data Controller shall communicate any rectification or erasure of Personal Data or restriction of Processing carried out following a Data Subject's request to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. In addition such BCR Member shall inform the Data Subject about those recipients if the Data Subject requests it.

7.5 Exercising Data Subjects' Rights

Data Subjects are entitled to enforce this BCR-C as third-party beneficiaries, and to exercise their rights with respect to the Processing of their Personal Data by any BCR Member acting as Data Controller. The BCR Member shall ensure that any request or complaint from Data Subject in relation to the exercise of their rights ("**Requests**") is addressed in a timely manner.

Data Subjects can make a request verbally or in writing. BCR Members will provide Data Subjects with accessible means to exercise their rights and, in particular:

1 - A single dedicated contact email to be used irrespective of the country a Data Subject is located in:

dpo@concentrix.com

Local emails can be used in order to take into account local specificities, such as language.

To reach out your local privacy contact, please refer to Appendix 01 - List of Concentrix entities bound by the BCR-C and local Privacy email contacts.

2 - Single portal with Concentrix DPO email address accessible on www.concentrix.com

3 - Single dedicated postal address to be used irrespective of the country a Data Subject is located in:

Group Data Privacy Officer

Legal and Compliance Department

3 rue d'Heliopolis

75017 – PARIS

FRANCE

The DPO, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the Requests, shall (i) ensure that they have obtained the minimum required information from the concerned Data Subject to address his/her Request (ii), if deemed necessary, obtain as much information as possible to enable the Request to be duly handled.

If there is a doubt about the identity of the individual making the request, mainly when using distance communication means, a BCR Member may be required to ask for more information regarding the Data Subjects. Information collected shall be (i) limited to information that is necessary to confirm who the individual making a request is and (ii) shall not be collected when products or services provided by a BCR Member or its Clients are not delivered under the real identity of the user. Proportionality shall always be assessed by the Data Controller.

In any case, the response to a Data Subject must occur within 1 month at the latest after receiving the Request. Taking into account the complexity and number of the requests, that one-month period may be extended at maximum by two further months, in which case the complainant should be informed accordingly (as detailed in Appendix 5).

Where the Data Subject is not satisfied with the initial response provided by the BCR Member such Data Subject shall be entitled in any case to immediately ask for his or her Request to be re-examined. Data Subject shall provide to the BCR Member a detailed explanation of the unsatisfactory provisions of the solution previously provided. The BCR Member shall take no longer than 2 months from receipt of the Request for re-examination to determine how it shall be handled and shall inform the Data Subject in writing accordingly.

If a Data Subject Request or complaint is rejected by the BCR Member or the answer does not satisfy the Data Subject or in any case, the Data Subject can contact the DPO and / or can directly lodge a complaint with a competent EEA Supervisory Authority and / or can seek judicial remedy as further detailed above in section 7.1 and 7.2 above.

Further details regarding this Article are available in the following appendix:

- **Appendix 5 - Procedure for Data Subjects' requests where Concentrix acts as Data Controller**

8. Data Subjects complaint handling procedure

Data Subjects are entitled to lodge a complaint directly to a BCR Member regarding the Processing of Personal Data they consider non-compliant with this BCR-C before the BCR Member they deem to be non-compliant. Where the breach is likely to result from an act of a BCR Member located outside the EEA, the Data Subject can lodge the complaint directly before Concentrix SAS as the European Lead Entity.

Data Subjects may raise a complaint by:

(1) Contacting the relevant Local Privacy Leader of the relevant BCR Member by email at the address is provided in Appendix 01 of the BCR-C, and/or

Contacting the Group Data Privacy Officer at dpo@concentrix.com or by mail at 3/5 rue d'Heliopolis, 75017, Paris, France.Such complaint will be handled by the relevant BCR Member(s) in due course and with particular care and attention according to the steps and timing defined herein. Such provisions are also applicable in relation to Data Subjects requests to exercise their rights (see Article 7 above).

In practice, complaints made by Data Subjects will be handled according to the procedure defined under **Appendix 5 - Procedure for Data Subjects' requests where Concentrix acts as Data Controller**.

The BCR Member acting as Data Controller shall provide information on actions taken to the Data Subject / complainant without undue delay, and in any event within one month from the date such complaint is lodged in accordance with the provisions herein. The Complaint shall be handled by a clearly identified department or person with an appropriate level of independence in the exercise of their functions. In practice, the relevant department or person shall be the Legal & Compliance department (more particularly, the relevant Geo Compliance Officer and/or the Local Privacy Leader). Taking into account the complexity and number of the requests, that one-month period may be extended at maximum by two further months, in which case the complainant should be informed accordingly.

In the event the relevant BCR Member decides to reject a complaint made by a Data Subject, such BCR Member undertakes to inform the Data Subject about its decision and to provide him/her with information regarding the reason for such dismissal.

In the event a BCR Member considers that a complaint made by a Data Subject is justified, such BCR Member commits to implement the corrective measures it deems adequate to remedy such situation as soon as reasonably possible. In addition, the BCR Member will also inform the concerned Data Subject once the corrective measures have been implemented and the situation is remedied.

In any case, BCR Members acknowledge that Data Subjects remain entitled to lodge a claim before an EEA Supervisory Authority and / or to seek judicial remedy.

BCR Members further acklowledge that such rights is not dependent on the Data Subjects having used the complaint handling process beforehand, although Data Subjects re encourage to do so.

9. Data protection governance

Concentrix has defined a Data protection organisation and governance which is further defined under Appendix 3.

BCR Members undertake to designate a Data Protection Officer, where required and in line with Article 37 GDPR, or any other person or entity (such as a chief privacy officer) with responsibility to monitor compliance with the BCR-C and enjoying the highest management support for the fulfilling of this task. This organisation is led by the Group Data Privacy Officer who relies on a network of privacy contact points (namely Regional Privacy Leaders, Local Privacy Leaders as well as Business Privacy Referents) and who may be designated as DPO by the relevant BCR Member.

The DPO formally appointed with a Supervisory Authority shall directly report to the highest management level. In addition, the DPO can inform the highest management level if any questions or problems arise during the performance of their duties.

The DPO should not have any tasks that could result in conflict of interests. The DPO should not be in charge of carrying out data protection impact assessments, neither should they be in charge of carrying out the BCR audits if such situations can result in a conflict of interests. However, the DPO can play a very important and useful role in assisting the BCR Members, and the advice of the DPO should be sought for such tasks.

The roles and responsibilities of the network as well as its working governance are further defined under **Appendix 3 – Data Protection organization and governance**

In addition, the DPO can inform the highest management level if any questions or problems arise during the performance of their duties.

The DPO and the Regional and/or Local Privacy Leaders may be contacted at the contact details described in Article 7.5 of the BCR-C and at the local privacy contacts provided in Appendix 01 of the BCR.

10. Training and awareness

Protecting Personal Data is not only a matter of compliance with privacy laws but is part of the embodiment of Concentrix core values. In this context, fostering a privacy culture within the group is essential to make all employees, trainees, and other persons whose conduct in the performance of work is under the direct control of BCR Members accountable for the protection of Personal Data Processed as part of their operations.

Therefore, this BCR-C shall be properly implemented within the whole organisation. To this end, BCR Members have adopted a privacy training program which aims at ensuring that Concentrix employees, trainees, and other persons whose conduct, in the performance of work is under the direct control of BCR Members, are actually aware of the obligations, principles and procedures specified under this BCR-C. In addition to the key GDPR principles and obligations, the training and awareness programme shall cover, among others, procedures for managing requests for access to personal data by public authorities

Such training is aimed at: (i) individuals having permanent or regular access to Personal Data; (ii) individuals involved in the collection of Personal Data; and/or (iii) individuals involved in the development of tools used to process Personal Data.

The training material shall be up-to-date and regularly reviewed, at least annually or upon significant changes in the applicable Data Protection Legislation, in order to ensure it reflects the latest verison of the BCR-C.

The training program will aim at providing:

- A basic level of core knowledge regarding the applicable principles when Processing Personal Data and a good understanding of the existing procedures and their implementation; and,
- Specific training adapted to the different functions within the organisation.

In this regard it is reminded that BCR Members acknowledge no transfer can be made under the BCR-C to another BCR Member, unless the latter is effectively bound by the BCR-C and appropriate training on the BCR-C can effectively be provided to the employees of the respective BCR Member.

BCR Members undertake to ensure that all Concentrix employees, trainees, and other persons whose conduct, in the performance of work is under the direct control of BCR Members, take the training upon arrival and subsequently complete a refresh every year.

Further details regarding this Article are provided in the following appendix:

- **Appendix 04 – Privacy awareness and training program**

11. Privacy by design/privacy by default

In order to ensure that the principles defined under this BCR-C are effectively taken into account and reflected in the different Processing it carries out, Concentrix will take data protection into consideration and implement appropriate technical and organizational measures from the very beginning of any new project.

In order to provide a high level of protection to the Personal Data within the organisation, the principles and obligations defined hereunder will thus be integrated into the design of each project on the basis of privacy by design procedures adopted by Concentrix.

12. Transparency and cooperation

12.1 Communication of the BCR-C

BCR Member commit to ensure that all Data Subjects will be provided with information on their third-party beneficiary rights, with regard to the processing of their Personal Data, and on the means to exercise those rights. Such information is described in Article 7 of the BCR-C.

Concentrix will openly communicate this BCR-C to the Data Subjects and make it easily accessible to any individual. Such communication shall allow any Data Subject to obtain a copy of this BCR-C with no undue delay and in an open format. In addition, a public version of the latest version of the present BCR-C shall be available at any time to Data Subjects on Concentrix website www.concentrix.com. Data Subjects may also request a copy of the BCR-C by contacting the DPO at dpo@concentrix.com.

The public version of the BCRs-C shall at least contain the following information:

- A description of the scope of the BCR-C (Article 2 of the BCR-C),
- The clause relating to the Group's liability (Article 7 of the BCR-C),
- The clauses relating to the data protection principles (Article 4, 4.1, 4.2, 4.3, 4.5, 4.6, 4.7, 4.9 , 4.10 and 5 of the BCR-C),
- The lawfulness of the processing (Articl 4.1 and 5 of the BCR-C),
- Security and personal data breach notifications (Article 4.7 and 4.10 of the BCR-C),
- Restrictions on onward transfers (Article 4.9 and Article 6 of the BCR-C), and
- The clauses relating to the rights of the data subjects (Article 7, 8 and 12 of the BCR-C).

This information should be up-to-date, and presented to Data Subjects in a clear, intelligible, and transparent way. This information should be provided in full, hence a summary hereof will not be sufficient

The public version shall also include all required policies and procedures attached to the BCR-C as an Appendix, especially for BCR-C:

- Appendix 01 - A List of BCR Members bound by the BCR-C and local privacy email contacts
- Appendix 02 Definitions for BCR and Procedures
- Appendix 05 Procedure for Data Subjects' requests where Concentrix acts as Data Controller
- Appendix 11-A BCR-C material scope: List of Purposes of Processing and related Categories of Personal Data and Data Subjects

The other Apppendices are either not applicable to the BCR-C or are internal processes not relevant for Data Subjects to understand and/or exercize their rights.

This above requirements will be met by ensuring that that a simplified public version of the BCR-C containg all information previously listed is available on Concentrix website (www.concentrix.com).

Concentrix will promote the improvement of the privacy and security culture within its organisation by sharing this BCR-C through internal systems and means (e.g., Concentrix Intranet, internal communications, etc.).

12.2 Information to Data Subjects

BCR Members, where acting as Data Controller shall provide Data Subjects any information required by the Applicable Data Protection Legislation. The BCR Member will provide such information without delay and within a reasonable period after obtaining the Personal Data, but at the latest within one month, at the time of first communication or first disclosure with a legitimate recipient. Such information shall be composed at least of the following elements:

- The identity and the contact details of the Data Controller;
- The contact details of the data protection officer (DPO) and/or the Local Privacy Leader;
- The purposes of the Processing and its legal basis;
- If the information is not collected directly from the Data Subject, the categories of Personal Data Processed;
- The recipients of the Personal Data;
- Where applicable, the existence of Data Transfers outside of the EEA, the countries where the Personal Data is transferred to, the measures implemented to ensure an adequate level of protection and the means by which to obtain a copy of them or where they have been made available;
- The data retention period;
- The rights of the Data Subjects as defined under Article 7 above. (e.g. the existence of the right to request from the Data Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability);
- The right to lodge a complaint before a supervisory authority;
- Where Personal Data is collected from the Data Subject, whether the Data Subject (1) is obliged to provide the Personal Data due to any statutory or contractual requirement, or (2) has a requirement to provide the Personal Data as it is necessary to enter into a contract, and of the possible consequences of failure to provide such data;
- If the Processing is based on the consent of the Data Subjects, the right for them to withdraw their consent at any time without affecting the lawfulness of Processing based on consent before its withdrawal;
- If the Processing is based on the BCR Member's legitimate interest, explanations regarding said legitimate interest;
- As the case may be, the existence of automated decision-making, including profiling; and
- Where the Personal Data is not collected from the Data Subject, any available information as to their source (e.g. in particular, categories of Personal Data, source from which the Personal Data originates, public nature of the Personal Data);

BCR Members undertake to provide such information to Data Subjects in accessible, easy to understand, clear and in plain and simple language

12.3 Inconsistencies with local legislations & practices affecting compliance with BCR-C

BCR Members commit to use the BCR-C as a tool for Transfers only where they have assessed that the law and practices in a Non-Adequate third country of destination applicable to the Processing of the Personal Data by the BCR Member acting as Data Importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under these BCR-C.

Such commitment is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the below listed purposes are not in contradiction with the BCR-C:

(a) national security, and/or,
(b) defence, and/or
(c) public security, and/or
(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; and/or
(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; and/or
(f) the protection of judicial independence and judicial proceedings; and/or
(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; ad/or
(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); and/or
(i) the protection of the Data Subject or the rights and freedoms of others; and/or
(j) the enforcement of civil law claims.

In assessing the laws and practices of the Non-Adequate Third Country which may affect the respect of the commitments contained in the BCR-C, the BCR Members shall take due account, in particular, of the following elements:

- **The specific circumstances of the Transfers** or set of Transfers, and of any envisaged onward Transfers within the same third country or to another Non-Adequate Third country, including:
  - purposes for which the Personal Data are transferred and Processed (e.g. marketing, HR, storage, IT support, clinical trials);
  - types of entities involved in the Processing (the Data Importer and any further recipient of any onward Transfer);
  - economic sector in which the Transfer or set of Transfers occur;
  - categories and format of the Personal Data Transferred;

  - location of the Processing, including storage; and
  - transmission channels used.
- **The laws and practices of the third country of destination** relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these Personal Data during the transit between the country of the Data Exporter and the country of the Data Importer, as well as the applicable limitations and safeguards.
- **Any relevant contractual, technical or organisational safeguards** put in place to supplement the safeguards under the BCR-C, including measures applied during the transmission and to the Processing of the Personal Data in the country of destination.

Where any safeguards in addition to those envisaged under the BCR-C should be put in place, Concentrix SAS, as the Liable BCR Member, the DPO and the relevant Local Privacy Leader will be informed and involved in such assessment.

BCR Members shall document appropriately such assessment, as well as the supplementary measures selected and implemented. Such documentation shall be made available to the competent Supervisory Authority and to the DPO upon request.

In addition, BCR Member acting as Data Importer shall promptly notify the Data Exporter if, when using these BCR-C as a tool for Transfers, and for the duration of the BCR membership, it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCR-C, including following a change in the laws in the Non-Adequate Third Country or a measure (such as a disclosure request). This information should also be provided to the Liable BCR Member and to the DPO.

Upon verification of such notification, the BCR Member acting as Data exporter, along with the Liable BCR Member, and with the assistance of the DPO, the relevant Local Privacy Leader and the Information Security team, should commit to promptly identify supplementary measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the BCR Member acting as Data Exporter and/or Data Importer, in order to enable them to fulfil their obligations under the BCR-C. The same applies if a BCR Member acting as Data Exporter has reasons to believe that a BCR Member acting as its Data Importer can no longer fulfil its obligations under this BCR-C.

Where the BCR Member acting as Data Exporter (along with the Liable BCR Member and the DPO and/or the relevant Local Privacy Leader) assesses that the BCR-C, even if accompanied by supplementary measures, cannot be complied with for a Transfer or set of Transfers, or if instructed by the competent Supervisory Authority, such BCR Member commits to suspend the Transfer or set of Transfers at stake, as well as all Transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the Transfer is ended.

Following such a suspension, the BCR Member acting as Data Exporter has to end the Transfer or set of Transfers if the BCR-C cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, Personal Data that have been transferred prior to the suspension, and any

copies thereof, should, at the choice of the BCR Member acting as Data Exporter, be returned to it or destroyed in their entirety.

Concentrix SAS, as the liable BCR Member and the DPO and/or the relevant Local Privacy Leader, will inform all other BCR Members of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of Transfers is carried out by any other BCR Member or, where effective supplementary measures could not be put in place, the Transfers at stake are suspended or ended.

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

12.4 Duty to cooperate

In any event, BCR Members agree to cooperate with EEA Supervisory Authorities, including by accepting to be audited or inspected (onsite on remotely) by such Supervisory Authorities, to take into account the advice, and to abide by decision of the competent EEA Supervisory Authority that may be provided in relation to this BCR-C. BCR Members acknowledge and agree that the competent Supervisory Authority powers and audit rights cannot be limited, in particular in relation to the practical audit conducted by such Supervisory Authority.

BCR Members, and where applicable, their respective representative shall make available to the EEA Supervisory Authority, upon request, any information about the processing operations covered by the BCR-C, such as the records of processing activities.

Any dispute related to the competent Superviroy Authority's exercise of supervision of compliance with the BCR-C will be resolved by the courts of the Member State of that Supervisory Authority, in accordance with that Member State's procedural law. The BCR Members agree to submit themselves to the jurisdiction of these courts.

13. Audit programme covering the BCR

Each BCR Member acting as Controller shall be responsible for and able to demonstrate compliance with the BCR-C. To his end, and in addition with the requirements set out in Article 4.4 (Holding a Record), 4.8 (Data Protection Impact Assessment) and Appendices 08 – Personal Data breach Notification, BCR Members shall comply with the following requirement reagrding data protection audit programme.

BCR Member commit to develop and integrate into its audit program the review of its compliance with this BCR-C. The audit program will enable to define:

- a reasonable frequency according to which audits shall be carried out;
- the expected scope of the audit; and
- the team in charge of the audit.

The audit procedure is detailed in **Appendix 7 – Procedures for Data Privacy Audits**. The audit covers all aspects of this BCR-C (for instance, applications, IT systems, databases that process personal data, or onward transfers, decisions taken as regards mandatory requirements under national laws that conflict with the BCR-C, review of the contractual terms used for the transfers out of the Group to controllers or processors of data, corrective actions, etc.), including methods and action plans ensuring that corrective actions will take place. However, such audit programme does not necessarily need to monitor all aspects of the BCR-C each time a BCR Member is audited, as long as all aspects of the BCR-C are monitored at appropriate regular intervals for that BCR Member.

BCR Members commit to have audits conducted on a regular basis (at least annually and/or if there are indications of non-compliance) to ensure verification of compliance with the BCR-C or considering the risk level of a Processing activity covered by the present BCR-C to the rights and freedoms of Data Subjects.

In addition to the regular audits, specific audits (ad hoc audits) may be requested by the DPO and/or the relevant privacy network member (e.g. the Local Privacy Leader), or any other competent function in Concentrix group such as the internal audit department. Such audits may be conducted by either internal and/or external accredited auditors advised by the DPO and/or the relevant privacy network member. The roadmap is initiated and determined by the DPO and/or the relevant privacy network member, as specified in Appendix 7. In any case, external auditors shall be independent and bound by a confidentiality obligation and/or be under an appropriate statutory obligation of confidentiality.

The DPO is responsible for determining the scope of audits to be performed. To this end, it can consult the Privacy Committee and/or entrust the internal audit team of Concentrix to determine the scope of such audit. The audit may be conducted by the Group DPO and/or the relevant privacy network members (e.g., the Local Privacy Leader) and/or by the internal audit team of the Concentrix group or any other relevant functions within Concentrix provided that:

- the persons in charge are guaranteed independence as to the performance of their duties to these audits; and
- the persons in charge of auditing compliance with the BCR-C, if such situation result in a conflict of interests.

The results of each audit will be submitted to the Group DPO and/or the relevant privacy network members (e.g., Local Privacy Leaders) and/or the Privacy Committee and/or Concentrix SAS board members for information. The final report, defect identification and remedial actions are to be shared and enforced by the Local Privacy Leader. Based on the Local Privacy Leader assessment, the report may also be shared, where appropriate, to any Business Privacy Referent, local security manager, process / system owners, Concenrix group ultimate parent's board company or the board of the relevant BCR Member subject to the audit or any other required internal employee. Remedial actions will be defined with a prioritisation to determine a schedule for implementing such measures.

Concentrix acknowledges that competent EEA Supervisory Authorities can request communication of the audit results and thus agree to grant them access thereto upon request. The results of the audit reports and relevant internal audit reports will be maintained in a form that the Supervisory Authorities located in the EEA may access them if they utilize their audit right set out below.

BCR Members undertake to ensure that the Competent Supervisory Authorities can have access to the results of the audit upon request and shall not limit such rights, especially on grounds of confidentiality, e.g. related to the protection of business secrets

It is reminded BCR Member shall entitle any competent EEA Supervisory Authority to carry out data protection audits themselves on any issue related to the BCR-C. In this respect, each BCR Member shall permit the EEA Supervisory Authority to audit the relevant BCR Member in order that the EEA Supervisory Authority may obtain the information necessary to demonstrate BCR Member(s) compliance with this BCR-C (see also Article 12.4 above).

14. Change to the BCR-C

Concentrix DPO with the support of the Local Privacy Leaders will ensure that the present BCR-C is kept up to date (for instance to take into account modifications of the regulatory environment, EU data protection authorities recommendations, or changes to the scope of the BCR-C).

In particular, the DPO shall keep up to date a list of entities bound by the BCR-C. Where any new entity of Concentrix becomes effectively bound by the BCR-C (as specified in Article 3.2), the DPO shall update the list and shall inform without undue delay all BCR Members and the relevant EEA Supervisory Authorities via the competent EEA Supervisory Authority.Such updated information will be made available to Data Subjects together with the BCR-C and via the same means.

At least once a year, or when deemed necessary by the DPO, Concentrix SAS will report such changes to the competent EEA Supervisory Authorities. The notification of such changes to EEA Supervisory Authorities will be carried out at least once a year via the competent EEA Supervisory Authority with a brief explanation of the reasons justifying the update. The Supervisory Authorities should also be notified once a year, following the same process, in instances where no changes have been made.

The annual update or notification should also include the renewal of the confirmation regarding the fact that Concentrix SAS, as the Liable BCR Member made appropriate arrangements to enable itself payment of compensation for any damages resulting from the breach of the BCR-C by BCR Members outside the EEA.

To the same extent where an amendment has substantial impact on the BCR-C or on the level of protection of the rights granted by this BCR-C, Concentrix SAS, with the assistance of the DPO, undertakes to promptly inform BCR Members and EEA Supervisory Authorities.

15. Non-compliance with the BCR-C

By becoming a BCR Member, Data Exporter and Data Importer shall comply with the following requirements:

- No transfer is made to a BCR member unless the BCR member is effectively bound by the BCR-C and can deliver compliance.
- The Data Importer should promptly inform the Data Exporter if it is unable to comply with the BCR-C, for whatever reason, including the situations further described in Article 12.3 of the BCR-C above.
- Where the Data Importer is in breach of the BCR-C or unable to comply with them, the Data Exporter should suspend the Transfer (See also Article 12.3 of the BCR-C above) .

The Data Importer shall, at the choice of the Data Exporter, immediately return or delete the Personal Data that has been Transferred under the BCR-C in its entirety, where:

- The Data Exporter has suspended the transfer, and compliance with this BCR-C is not restored within a reasonable time, and in any event within one month of suspension; or
- The Data Importer is in substantial or persistent breach of the BCR-C; or
- The Data Importer fails to comply with a binding decision of a competent court or Competent SA regarding its obligations under the BCR-C.

The same commitments should apply to any copies of the data. The Data Importer should certify the deletion of the data to the Data Exporter.

Until the data is deleted or returned, the Data Importer should continue to ensure compliance with the BCR-C.

In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer should warrant that it will continue to ensure compliance with the BCR-C, and will only process the data to the extent and for as long as required under that local law.

For cases were applicable local laws and/or practices affect compliance with the BCR-C, see Article 12.3 of the BCR-C above.

16. Termination

A BCR Member acting as data importer, which ceases to be bound by the BCR-C may keep, return, or delete the Personal Data received under the BCR-C.

If the Data Exporter and Data Importer agree that the data may be kept by the Data Importer, protection must be maintained in line with Chapter V GDPR and as reflected in Article 6 of the BCR-C.

17. Appendices

- Appendix 01 - List of Concentrix entities bound by the BCR-P and local Privacy email contacts
- Appendix 02 - Definitions for BCRs and Procedures
- Appendix 03 - Not Provided
- Appendix 04 - Not Provided
- Appendix 05 - Procedure for Data Subjects' requests where BCR Members acts as Data Controller
- Appendix 06 - Not Provided
- Appendix 07 - Not Provided
- Appendix 08 - Not provided
- Appendix 09 - Not Provided
- Appendix 10 - Not Provided
- Appendix 11-A BCR-C List of Purposes of Processing and related Categories of Personal Data and Data Subjects (Material Scope)
- Appendix 11-B Not Provided

17.1 Appendix 01 - List of Concentrix entities bound by the BCR-P and local Privacy email contacts

Appendix 01

List of Concentrix entities bound by the BCR and local privacy email contacts

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
1.	Concentrix Albania Shpk	Rruga Dervish Hima, Stadiumi Air Albania, Qendra e Biznesit, Shkalla BC, nr.B-C, Niveli +3, 1019 Tirana	Albania	privacy.it@concentrix.comprivacy.it@concentrix.com
2.	Webhelp Algerie SPA	16bis, cité Bois des Cars 2 16047 Dely Ibrahim	Algeria	privady.dz@concentrix.com
3.	Concentrix Austria GmbH	Floridsdorfer Haptstrasse 1, 1210 Vienna	Austria	datenschutz@concentrix.com
4.	Concentrix Payment Services Benelux, SA (« CPS Benelux »)	Avenue Louise, 87 - 1050 Bruxelles	Belgium	privacy.cps@concentrix.com.
5.	Concentrix Benin	Immeuble le Jatoba, avenue Jean-Paul II, lot 20, zone résidentielle portuaire; (Nouveau site en cours : Parcelle F G Ilot 40002,quartier Enagnon Akpakpa Cotonou)	Bénin	Privacy.fr@concentrix.com
6.	Concentrix BH d.o.o. Sarajevo	Josipa Stadlera 6, 71000, Sarajevo	Bosnia-Herzegovina	datenschutz@concentrix.com
7.	Services Tech Experience Inovaçao e technologia em relacionamento Ltda	Rua Marechal Deodoro, 314 6th Floor, Sets 601-606, Centro Curitiba, Paraná, 80.010-01	Brazil	protecciondedatos@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
8.	Services Assessoria Digital Ltda	Rua Marechal Deodoro 314, 11th floor,Centro Curitiba, Paraná, 80.010-010	Brazil	protecciondedatos@concentrix.com
9.	Webhelp Bulgaria EOOD	Blvd. Totleben, Business-Center Sofia City-West 53-55, 1606, Sofia	Bulgaria	datenschutz@concentrix.com
10.	Les services Webhelp, Inc	880 Rue Roy Est, QC H2L 1E6, Montréal, Quebec	Canada	protecciondedatos@concentrix.com
11.	Concentrix (Suzhou) Data Services Co. Ltd	Unit 2605B, 26th Floor, West Tower, China Overseas Fortune Center, No. 9 Suzhou Avenue West, Suzhou Industrial Park	China	privacy.my@concentrix.com
12.	Concentrix CX Colombia SAS	Carrera 52 No. 65 91 OF 740 CENTRO COMERCIAL AVENTUR, Medellín	Colombia	protecciondedatos@concentrix.com
13.	Concentrix International Colombia SAS	Avenida carrera 19 # 28 80 Cc Empresarial Calima Of 401, Bogota	Colombia	protecciondedatos@concentrix.com
14.	Concentrix Experts Colombia SAS	Carrera 52 No. 65 61, Medellín	Colombia	protecciondedatos@concentrix.com
15.	Concentrix CRM Colombia SAS	Diagonal 55 No. 37 41 OF. 601	Colombia	protecciondedatos@concentrix.com
16.	Concentrix Servicios Colombia SAS	Diagonal 55 Av 37 41 OF 701, Bello	Colombia	protecciondedatos@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
17.	Concentrix Czech Republic , s.r.o	Vaclavske namesti 808/66, 11000 Praha, Nové Mesto	Czech Republic	privacy.cz@concentrix.com
18.	Concentrix Denmark, AS	Borgmester Christiansens Gade 50, 2, 2500, Copenhagen	Denmark	privacy.nordic@concentrix.com
19.	Webhelp Egypt, LLC	plot No. 53, First District, City Center New Cairo, Cairo	Egypt	privacy.eg@concentrix.com
20.	Onelink SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	protecciondedatos@concentrix.com
21.	Tetel SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	protecciondedatos@concentrix.com
22.	Getcom International SA de CV	Boulevard Los Próceres, Colonia Palermo Edificio Ex Panades, No. 350, Frente a UCA, San Salvador, San Salvador.	El Salvador	protecciondedatos@concentrix.com
23.	RH-T SA de CV	Avenida Albert Einstein y Bulevar, San Salvador.	El Salvador	protecciondedatos@concentrix.com
24.	Concentrix Estonia OÜ	Tartu mnt 63, Tallinn 10115	Estonia	privacy.nordic@concentrix.com
25.	Concentrix Finland, Oy	Palkkatilanportti 1 FI-0240 Helsinki	Finland	privacy.nordic@concentrix.com
26.	Concentrix Catalyst France SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell , 75017 Paris	France	Privacy.fr@concentrix.com
27.	Concentrix, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	Privacy.fr@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
28.	Concentrix Conseil France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	Privacy.fr@concentrix.com
29.	C Automobile Services, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell	France	Privacy.fr@concentrix.com
30.	Concentrix CX France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	Privacy.fr@concentrix.com
31.	Concentrix Caen, SAS	1 rue Jean Perrin, 14460 Colombelles	France	Privacy.fr@concentrix.com
32.	Concentrix Compiègne France, SAS	ZAC du Parc Tertiaire - 98 impasse Les Terres auprès des Iles, 60610, Compiègne	France	Privacy.fr@concentrix.com
33.	Conncentrix Fontenay-Le-Comte France, SAS	6 Rue de l'Innovation, 85200 Fontenay-le-Comte	France	Privacy.fr@concentrix.com
34.	Marnix French ParentCO, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	dpo@concentrix.com
35.	Marnix French TOPCO, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	dpo@concentrix.com
36.	Marnix, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	dpo@concentrix.com
37.	WowHoldCo, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	dpo@concentrix.com
38.	Concentrix Gray, SAS	ZAC GRAY SUD	France	privacy.fr@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		70100 GRAY		
39.	Concentrix Montceau France, SAS	16 rue Saint-Eloi, 71300, Montceau les Mines	France	privacy.fr@concentrix.com
40.	Concentrix Vitré France, SAS	Parc d'Activité Etrelles, 35370 Etrelles	France	privacy.fr@concentrix.com
41.	Concentrix University France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy.fr@concentrix.com
42.	Concentrix Prestations France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy.fr@concentrix.com
43.	CTG France, SAS	39 rue des métissages 59200 Tourcoing	France	privacy.fr@concentrix.com
44.	Concentrix Medica Customer Expérience France	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy.webhelpmedica@concentrix.com ; privacy.patientys@concentrix.com
45.	Patientys, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy.webhelpmedica@concentrix.com ; privacy.patientys@concentrix.com
46.	CGE France (Concentrix Grand-Est France, SAS)	Technopole, 9 rue Thomas Edison, Metz	France	privacy.fr@concentrix.com
47.	Concentrix Medica France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy.webhelpmedica@concentrix.com ; privacy.patientys@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
48.	Concentrix SFIA France, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy.fr@concentrix.com
49.	CCS, SAS	12 Rue Alfred Kastler 71530 Fragnes-La Loyere	France	privacy.fr@concentrix.com
50.	Netino, SAS	3/5 rue d'Héliopolis et 17/19 rue Guillaume Tell, 75017 Paris	France	privacy.fr@concentrix.com
51.	Solvencia, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy.cps@concentrix.com.
52.	ConcentrixO2C Holding, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy.cps@concentrix.com.
53.	Concentrix KYC Services, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy.cps@concentrix.com.
54.	ConcentrixPayment Services France, SAS	450 Rue Félix Esclangon, 73290 La Motte-Servolex	France	privacy.cps@concentrix.com.
55.	Concentrix Payment Services Deutschland, GmbH	Frankfurter Str. 151A, 63303 Dreieich	Germany	privacy.cps@concentrix.com.
56.	Webhelp Sun Holding GmbH	Tullnaustrasse 20, 90402, Nuremberg	Germany	datenschutz@concentrix.com
57.	Concentrix Holding Germany GmbH	Tullnaustrasse 20, 90402 Nuremberg	Germany	datenschutz@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
58.	Concentrix Deutschland GmbH	Tullnaustrasse 20, 90402 Nuremberg	Germany	datenschutz@concentrix.com
59.	RIGHTHEAD GmbH	Tullnaustrasse 20, 90402 Nuremberg	Germany	datenschutz@concentrix.com
60.	Concentrix CX Technologies Ltd	SU TOWER, N°18, Castle Road, North Ridge, Accra	Ghana	privacy.fr@concentrix.com
61.	Concentrix Greece Single Member Limited Company ('Concentrix Greece')	36 Voukourestiou Str 10673 Athens	Greece	privacy.gr@concentrix.com
62.	Concentrix Guatemala SA	15 Avenida 17-30 Zona 13, Oficina 201, Guatemala, Guatemala	Guatemala	protecciondedatos@concentrix.com
63.	Concentrix Solutions Guatemala SA	15 Avenida 17-40 zona 13, Torre 1, Nivel 1 Edificio Tetra Center, Ciudad de Guatemala	Guatemala	protecciondedatos@concentrix.com
64.	Concentrix Xperts Guatemala SA	15 Avenida 17-40 zona 13, Torre 1, Nivel 1 Edificio Tetra Center, Ciudad de Guatemala	Guatemala	protecciondedatos@concentrix.com
65.	Gobeyond Partners Asia Limited	31/F Tower Two Times Square 1, Matheson St., Causeway Bay, Hong Kong	Hong Kong	privacy.my@concentrix.com
66.	Concentrix India Private Ltd	Hindustan Times House, 10th Floor, 18-20 K G	India	privacy.uk@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		Marg, Connaught Place, New Delhi- 110001		
67.	SELLBYTEL Marketing Services India Private Ltd	Corporate Office:- Ground Floor, Tower A, SP Infocity, Udyog Vihar, Phase-1, Gurugram-122001, Haryana , India	India	privacy.uk@concentrix.com
68.	Concentrix Israel Ltd	Yigal Alon 94, Alon tower 1 Tel Aviv , Tel-Aviv	Israel	privacy.tr@concentrix.com
69.	Concentrix Payment Services Italia, SRL	Via Gozzano Guido 14 - 20092 Cinisello Balsamo	Italy	privacy.cps@concentrix.com.
70.	Concentrix Payment Services France (Italy branch)	Via Maurizio Gonzaga n° 7	Italy	privacy.cps@concentrix.com.
71.	Webhelp Enterprise Sales Solutions Italy	Via Torri Bianche, 7, 20871 Vimercate MB, Italy	Italy	privacy.it@concentrix.com
72.	Concentrix Cote d'Ivoire	Immeuble PIA, Avenue Abdoulay Fadiga, Plateau Abidjan - 01 BP 7171 ABJ 01	Ivory Coast	privacy.ci@concentrix.com
73.	Concentrix Le Workshop	Indenie, 6 rue des Sambas 01 BP 743 ABJ 01, Plateau Abidjan - 01 BP 743 ABJ 01	Ivory Coast	privacy.ci@concentrix.com
74.	privacy.ma@concentrix.com	Immeuble PIA, Avenue Abdoulay Fadiga,	Ivory Coast	privacy.ci@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		Plateau Abidjan - 01 BP 7171 ABJ 01		
75.	Webhelp Japan KK	Tokyo Club Building 11F, 3-2-6 Kasumigaseki, Chiyoda-ku, Tokyo	Japan	privacy.my@concentrix.com
76.	Webhelp Jordan LLC	Rafiq Al Hariri Ave 1, Amman	Jordan	privacy.jo@concentrix.com
77.	IQ-to-Link shpk	Rr. Ukshin Hoti nr. 121	Kosovo	datenschutz@concentrix.com
78.	Webhelp Kosovo L.L.C.	Rr. Ukshin Hoti nr. 120, 10000, Prishtina	Kosovo	datenschutz@concentrix.com
79.	Concentrix Latvia SIA	Raiņa Bulvāris, 11, Riga, LV-1050	Latvia	privacy.nordic@concentrix.com
80.	Concentrix Madagascar, SA (zone franche)	Bâtiment TITAN 2, Zone Galaxy Andraharo, Antananarivo 101	Madagascar	privacy.mg@concentrix.com
81.	Netino Madagascar	Lot II M92 Antsakaviro - Ambodirotra Cua Antananarivo 101 Analamanga	Madagascar	privacy.mg@concentrix.com
82.	Concentrix Malaysia Sdn. Bhd.	Menara Exchange 106, Level 6, Lingkaran TRX, Jalan Tun Razak, 55188 Kuala Lumpur, Malaysia	Malaysia	privacy.my@concentrix.com
83.	Onelink Mexico SA de CV	BOULEVARD 300 ENTRE CALLE CDA MEZTISOS - VILLAS DEL REY - CAJEME-OBREGÓN SONORA-	Mexico	protecciondedatos@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		MÉXICO, 85136, Ciudad Obregón		
84.	Onelink Servicios SA de CV	BOULEVARD 300 ENTRE CALLE CDA MEZTISOS - VILLAS DEL REY - CAJEME-OBREGÓN SONORA-MÉXICO, 85136, Ciudad Obregón	Mexico	protecciondedatos@concentrix.com
85.	Concentrix Maroc, SA	43 av Ibn Sina-Agdal-Rabat	Morocco	privacy.ma@concentrix.com
86.	Concentrix Succursale Maroc	28 Avenue Allal Ben Abdellah - (Business address: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy.ma@concentrix.com
87.	Concentrix Services, SA	15, Avenue Annakhil (Business address: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy.ma@concentrix.com
88.	Concentrix Contact Center, SA	N°50 BLOC F 11 IMMEUBLE AL FIDIAN I ET IMMEUBLE AL FIDIAN II AVENUE HASSAN I CITE DAKHLA (Business address: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy.ma@concentrix.com
89.	Concentrix Multimedia, SA	6, rue Lalla Nezha, 30000 Fès	Morocco	privacy.ma@concentrix.com
90.	Concentrix GRC, SA	43 Avenue Ibn Sina, 10000 Rabat	Morocco	privacy.ma@concentrix.com
91.	Concentrix Technopolis, SA	Agdal, 25, Rue Oued Al Makhazine (Business	Morocco	privacy.ma@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		adress: 43 av Ibn Sina-Agdal-Rabat)		
92.	Concentrix University Maroc, SARL	15 av Annakhil, (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy.ma@concentrix.com
93.	Concentrix Agadir, SA	Quartier Industriel, Avenue Hassan II, Immeuble Jaouhara (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy.ma@concentrix.com
94.	Concentrix Fès, SA	112 Avenue des FAR Champs de Course ville nouvelle (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy.ma@concentrix.com
95.	Concentrix Meknès, SA	Immeuble Angle Rue Badir Al Kobra et Rue Sebou angle rue Badr al Korba, Meknes (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy.ma@concentrix.com
96.	Concentrix Marrakech, SA	Quartier Industriel, Avenue Hassan II, Immeuble Jaouhara (Business adress: 43 av Ibn Sina-Agdal-Rabat)	Morocco	privacy.ma@concentrix.com
97.	Concentrix Afrique	CFC Bridge, lot 58, Rez de Chaussée (Core 1), quartier Casa-Anfa, Hay Hassani - Casablanca	Morocco	privacy.ma@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
98.	Concentrix Netherlands Holding, BV	Amersfoortsestraat 28, 3821CB, Amersfoort	Netherlands	privacy.nl@concentrix.com
99.	Customer Contact Management Group, BV	Amersfoortsestraat 28, 3821CB, Amersfoort	Netherlands	privacy.nl@concentrix.com
100.	Concentrix Nederland, BV	Koraalrood 50, 2718SC Zoetermeer	Netherlands	privacy.nl@concentrix.com
101.	Concentrix Netherlands CX Holding B.V.	Colosseum 42, 7521 PT Enschede	Netherlands	privacy.nl@concentrix.com
102.	Concentrix Netherlands CRM Services B.V.	Colosseum 42, 7521 PT Enschede	Netherlands	privacy.nl@concentrix.com
103.	Concentrix Netherlands Customer Contact Performance Group B.V.	Herengracht 501 H, 1017B, Amsterdam	Netherlands	privacy.nl@concentrix.com
104.	Xperts Nicaragua SA	Plaza El Sol 2 C. Sur, 1 C. Este, Casa No. 26, Los Robles Managua	Nicaragua	protecciondedatos@concentrix.com
105.	Concentrix CX NicaraguaSA	Barrio Largaespada. B. Largaespada Busto Jose Marti 3 C al Este 1 C al Norte, Managua	Nicaragua	protecciondedatos@concentrix.com
106.	Concentrix DOOEL Skopje	Bul. VMRO 1, 1000, Skopje, North-Macedonia	North-Macedonia	datenschutz@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
107.	Concentrix Norway, AS	Storgata 38, 0182 Oslo	Norway	privacy.nordic@concentrix.com
108.	Concentrix Norway Consulting AS	Storgata 38, 0182 Oslo	Norway	**privacy.nordic@concentrix.com**
109.	Webhelp Perù S.A.C.	Calle Santa Inés Nro. 115, Urbanización Industrial Santa Rosa, distrito Ate, Lima	Peru	protecciondedatos@concentrix.com
110.	Concentrix BPO Consulting Peru S.A.C.	Jirón Marcos Farfán, n° 3468, Lima	Peru	protecciondedatos@concentrix.com
111.	Webhelp Philippines, Inc.	12th floor, Makati Sky Plaza, 7788 Ayala avenue, Makati City, 1223	Philippines	privacy.my@concentrix.com
112.	Webhelp Poland Sp. z.o.o.	Ul. Taneczna 30, PL 02-829, Warszawa	Poland	datenschutz@concentrix.com
113.	ConcentrixSun Portugal, Unipessoal, Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2, 2470-296 Porto Salvo, parish of Porto Salvo, Oeiras	Portugal	privacy.pt@concentrix.com
114.	ConcentrixOeiras, Lda	Avenida Professor Cavaco Silva, Tagus Park, Edificio Qualidade, bloco A-2, Lisboa	Portugal	privacy.pt@concentrix.com
115.	Concentrix Lisboa, Unipessoal, Lda	Avenida D. João II, n° 43, Torre Fernão de Magalhães, 15° Piso,	Portugal	privacy.pt@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		freguesia de Parque das Nações, 1998-025, Lisboa		
116.	Concentrix SAS Succursal em Portugal	Avenida D. João II, nº 43, Torre Fernão de Magalhães, 15º Piso, freguesia de Parque das Nações, 1998-025 Lisboa	Portugal	privacy.pt@concentrix.com
117.	ConcentrixNorte, Unipessoal LDA	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, LIsboa	Portugal	privacy.pt@concentrix.com
118.	Webhelp New Generation Lisbon	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy.pt@concentrix.com
119.	Concentrix SFIA, Sucursal em Portugal	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy.pt@concentrix.com
120.	Concentrix Payment Services Espana, Sucursal em Portugal	Av. Mediterrâneo 1, 1990-203 Lisboa, freguesia de Parque das Nações, 1998-025, Lisboa	Portugal	privacy.cps@concentrix.com.
121.	Webhelp Romania SRL	Sector 1, Str. Doctor Iacob Felix, nr. 63-69, et. 2	Romania	privacy.ro@concentrix.com
122.	Concentrix Catalyst Romania S.A.	Strada Câmpul Pâinii nr.3-5, etajul 3	Romania	privacy.ro@concentrix.com
123.	Concentrix Senegal SASU	Almadies, Pointe des Almadies, en face King Fahd, fahd Palace, 284, TF nº284/NGA Dakar	Senegal	privacy.sn@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
124.	Webhelp SAS Succursale Senegal	Almadies, Imm Serenity Pointe des Almadies, en face King Fahd, fahd Palace TF n°284/NGA Dakar	Senegal	privacy.sn@concentrix.com
125.	Concentrix d.o.o Beograd	Makedonska 30, III. Floor, 11000, Beograd	Serbia	datenschutz@concentrix.com
126.	Webhelp Singapore Pte Ltd	9 Raffles Place, #26-01 Republic Plaza, Singapore 048619	Singapore	privacy.my@concentrix.com
127.	Concentrix Slovakia, s.r.o.	Staromestská 3 811 03, Bratislava - mestská časť Staré Mesto	Slovakia Republic	privacy.it@concentrix.com
128.	Webhelp Holding Germany GmbH (Slovenia Branch)	City Centre - Republic square, 1000, Ljubljana	Slovenia	datenschutz@concentrix.com
129.	Concentrix SA Outsourcing) Pty Ltd	19 Ameshoff Street, Braamfontein, Johannesburg, 2001	South-Africa	privacy.uk@concentrix.com
130.	Webhelp SAS, Sucursal en Espana	Plaza Solymar s/n, Edificio Benalmar ,29630 Benalmádena, Málaga	Spain	**privacy.es@concentrix.com**
131.	Direct Medica Iberica S.L.	CL LAGASCA, 95, 28006 MADRID	Spain	privacy.webhelpmedica@concentrix.com
132.	Concentrix Spain NWE	Plaza Solymar s/n Edificio WEBHELP, 29630 Benalmádena, Málaga	Spain	privacy.es@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
133.	Concentrix Payment Services Espana SA	Calle Vallespir, número 19, módulo 3, planta 1ª de Sant Cugat del Vallès	Spain	privacy@wps.webhelp.fr
134.	Concentrix Spain Business Process Outsourcing S.L.U	Avda. Diagonal 197 Barcelona, 08018	Spain	privacy.es@concentrix.com
135.	Concentrix Spain Holding SLU	Av. Diagonal 97, 12 Barcelona 08018	Spain	privacy.es@concentrix.com
136.	Telenamic N.V	Zonnebloemstraat 50, Paramaribo	Suriname	privacy.sr@concentrix.com
137.	ConcentrixSweden AB	Box 4006, 16904 Solna	Sweden	
138.	Concentrix IT Services AB	Box 4006, 16904 Solna	Sweden	privacy.nordic@concentrix.com
139.	Concentrix Schweiz AG	Richtistrasse 5, 8304 Wallisellen	Switzerland	datenschutz@concentrix.com
140.	Concentrix CX (Thailand) Co., Ltd	87/1 Capital Tower All Seasons Place, Unit 1604-6 Floor 16, Pathumwan District, 10330, Bangkok	Thailand	privacy.my@concentrix.com
141.	Concentrix Müşteri Hizmetleri A.Ş. (Concentrix Customer Services A.Ş – Main Entity.)	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42 Kağıthane İstanbul	Turkey	privacy.tr@concentrix.com
142.	Concentrix Müşteri Hizmetleri A.Ş. Bingöl Şubesi (Concentrix Customer Services INC. Bingöl Branch)	Recep Tayyip Erdoğan Mh. Aydınlık Cd. Bingöl Üniversitesi Fen Edebiyat Fakültesi	Turkey	privacy.tr@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
		Zemin Kat Merkez Bingöl		
143.	Concentrix Müşteri Hizmetleri A.Ş. Izmir Şubesi (Concentrix Customer Services INC. Izmir Branch))	Sakarya Mah. Akçay Cad. No:99/3 Gaziemir İzmir	Turkey	privacy.tr@concentrix.com
144.	Concentrix Müşteri Hizmetleri A.Ş. Izmir 2 (Concentrix Customer Services INC Izmir 2 Branch)	Sakarya Mah. Akçay Cad. No:99/3 Gaziemir İzmir	Turkey	privacy.tr@concentrix.com
145.	Concentrix Müşteri Hizmetleri A.Ş. Van 2 Şubesi (Concentrix Customer Services	Vali Mithat Bey Mah. Cemaller Sok. Roza Apt. Sitesi No:9A İpekyolu Van	Turkey	privacy.tr@concentrix.com
146.	Concentrix Müşteri Hizmetleri A.Ş. Van Şubesi (Concentrix Customer Services INC. Van Branch)	Vali Mithat Bey Mah. İskele Cad. No:51 İpekyolu Van	Turkey	privacy.tr@concentrix.com
147.	Concentrix Müşteri Hizmetleri A.Ş. Van 3 Şubesi (Concentrix Customer Services INC. Van 3 Branch)	Vali Mithat Bey Mah. İskele Cad. No:51 İpekyolu Van	Turkey	privacy.tr@concentrix.com
148.	Concentrix Müşteri Hizmetleri A.Ş. Ümraniye Şubesi (Concentrix Customer Services INC Umraniye Branch)	Fatih Sultan Mehmet Mahallesi Balkan Cad. Casper Plaza İş Merkezi Apt. No: 47/1 Ümraniye / Istanbul	Turkey	privacy.tr@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
149.	Concentrix Müşteri Hizmetleri A.Ş. Maltepe Şubesi (Concentrix Customer Services INC. Maltepe Branch)	Cevizli Mah. Tugay Yolu Cad. No.10CF Maltepe/İstanbul	Turkey	privacy.tr@concentrix.com
150.	Concentrix Müşteri Hizmetleri A.Ş. Bursa Şubesi (Concentrix Customer Services INC. Bursa Branch)	Panayır Mahallesi 3. Pınar Cad. No:345 B Osmangazi/ 16250 Bursa	Turkey	privacy.tr@concentrix.com
151.	Concentrix Müşteri Hizmetleri A.Ş. Ankara Şubesi (Concentrix Customer Services INC. Ankara Branch)	Kızılırmak Mah. Dumlupınar Bulvarı A Blok No:9A/810	Turkey	privacy.tr@concentrix.com
152.	Bin Çağrı Hizmetleri A.Ş. Main Entity (Bin Call Services Joint Stock Company)	Selahaddin-i Eyyübi Mah. Üniversite Cad. Fen Edebiyat Fakültesi No: Blok No:1/3a Merkez Bingöl	Turkey	privacy.tr@concentrix.com
153.	Concentrix İnsan Kaynakları Danışmanlık ve Destek Hizmetleri A.Ş. (Concentrix Human Resource Consultancy and Support Services A.ŞINC – Main Entity .)	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42,; Kağıthane - Istanbul	Turkey	privacy.tr@concentrix.com
154.	Teknofix Telekomünikasyon	Aydınevler Mah. Aslanbey Cad. No:1 D:5-	Turkey	privacy.tr@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
	ve Bilişim Hizmetleri San ve Tic A.Ş. Main Entity (Teknofix Telecomunication and Information Services Joint Stock Company)	6, Küçükyalı, Maltepe, Istanbul		
155.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri San ve Tic A.Ş. Kagithane Subesi (Teknofix Telecomunication and Information Services Joint Stock Company Kagıthane Branch)	Merkez Mh. Ayazma Cd. Papirus Plaza No.37/42, Kağıthane - Istanbul	Turkey	privacy.tr@concentrix.com
156.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri San ve Tic A.Ş. Ankara Basinevleri Subesi (Teknofix Telecomunication and Information Services Joint Stock Company Ankara Basinevleri Branch)	Basınevleri Mah. Yankılar Sok. No:16 Keçiören, Ankara	Turkey	privacy.tr@concentrix.com
157.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri San ve	Aydınevler Mah. Aslanbey Cad. No:1 D:5-6 Küçükyali Maltepe İstanbul	Turkey	privacy.tr@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
	Tic A.Ş. Antalya Şubesi (Teknofix Telecomunication and Information Services Joint Stock Company Antalya Branch)			
158.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri San ve Tic A.Ş. İzmir Şubesi (Teknofix Telecomunication and Information Services Joint Stock Company Izmır Branch)	Bostanlı Mah. Nebil Susup Sk. No:147 A Karşıyaka İstanbul	Turkey	privacy.tr@concentrix.com
159.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri San ve Tic A.Ş. Ankara Şubesi (Teknofix Telecomunication and Information Services Joint Stock Company Ankara Branch)	Emrah Mah. Basın Cad. No:131 B Keçiören Ankara	Turkey	privacy.tr@concentrix.com
160.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri San ve	Bağlarbaşı 1. Sedir Onyx Offices No:10/15 Osmangazİ Bursa	Turkey	privacy.tr@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
	Tic A.Ş. Bursa Şubesi (Teknofix Telecomunication and Information Services Joint Stock Company Bursa Branch)			
161.	Teknofix Telekomünikasyon ve Bilişim Hizmetleri San ve Tic A.Ş. Van Şubesi (Teknofix Telecomunication and Information Services Joint Stock Company Van Branch)	Vali Mithat Bey Mah. İskele Cad. No:39A İpekyolu Van	Turkey	privacy.tr@concentrix.com
162.	Concentrix TSC UK Ltd	11 Central Park Avenue, Central Business Park, Larbert, Falkirk, FK5 4RX,	United-Kingdom	privacy.uk@concentrix.com
163.	Concentrix Payment Services UK Ltd	C/o Civvals Limited, 50 Seymour Street, London W1H 7JG	United-Kingdom	privacy.cps@concentrix.com.
164.	Concentrix Medica UK Limited	Building 2, 1 Nunnery Square, S2 5DD, Sheffield	United-Kingdom	privacy.webhelpmedica@concentrix.com
165.	Webhelp USA Group Inc	1111 Brickell Avenue, Suite 11, FL 33131, Miami	USA	protecciondedatos@concentrix.com
166.	Webhelp USA LLC	1111 Brickell Avenue, Suite 11, FL 33131, Miami	USA	protecciondedatos@concentrix.com

#	Concentrix Entity (BCR Members)	Mailing address	Country	Privacy email address Reminder: you may also contact the Group DPO at any time at dpo@concentrix.com
167.	Concentrix Logbox USA	110 West 40th Street , Suite 1903 New York, NY 10018	USA	protecciondedatos@concentrix.com
168.	Webhelp Americas LLC	80 SW 8TH ST, SUITE 2900, FL 33130, Miami	USA	protecciondedatos@concentrix.com

17.2 Appendix 02 - Definitions for BCRs and Procedures

"Applicable Data Protection Legislation"	Means in the following order of prevalence (i) the European Regulation 2016/679 relating to the Processing of Personal Data as of its date of application ("GDPR"), (ii) EU Member States national laws and regulations relating the Processing of Personal Data and implementing GDPR and (iii) any regulation relating to the Processing of Personal Data applicable during the term of this Privacy Policy.
"Binding Corporate Rule" or BCR	Means Personal Data protection policies and procedures which are adhered to by BCR Members for transfers or a set of transfers of Personal Data to a Data Controller or Data Processor in one or more third countries within the Concentrix group.
"BCR Member"	Means any affiliate of the Concentrix group that signed and bound b y the thhe BCR-C and/or BCR-P and as such committed to comply with such BCR, BCR Members are listed in Appendix 01 of such BCR-C and BCR-P.
"Client"	Means any third party, contracting with Concentrix and acting as Data Controller, whose Personal Data is Processed by a BCR Member acting as Data Processor accordingly with its documented instructions.
"Competent SA" or "Competent Supervisory Authority"	Means the EEA Supervisory Authority for the Data Exporter
"Data" or "Information"	Means any kind of information which is individually accessible by electronic or other means such as, but not limited to, logs, Personal Data, documents or other materials.
"Database"	Means a collection of independent works, data, Information or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.
"Data Exporter"	Means the Data Controller or Data Processor Transferring the Personal Data to a non-EEA third country
"Data Importer"	Means the Data Controller or Data Processor receiving the Personal Data
"Data Controller" or "Controller"	Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determine the purposes and means of the Processing of Personal Data.
"Data Processor" or "Processor"	means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.
"Data Subject"	Means any natural person, who can be identified, directly or indirectly, by means reasonably likely to be used by any natural

	or legal person, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
"Device"	Means any Programmable object that can automatically perform a sequence of calculations or other sequence of operations on Data once programmed directly or indirectly for the task. Any electronic apparatus adapted for displaying in a readable format, Information. Devices include but are not limited to computers, smartphone, tablets, laptops, servers, Networks, telephony platforms etc.
EEA	Means the European Economic Area. Countries that are part of the EEA are the EU Member States as well as Iceland, Liechtenstein and Norway.
"EEA Supervisory Authority"	Means an independent public data protection authority which is established in an EEA Member State.
"Encryption"	Means a process to obfuscate data by transforming Data into a form in which there is a low probability of assigning a meaning or making it readable except when used in conjunction with a confidential process or key to decode it. Such process could be, but are not limited to mathematical function or algorithmic process
"Information Administrator"	Means the natural person within Concentrix organisation, alone or jointly with others, processes or manipulates the Information in accordance with the Information Owner needs', the objectives', purposes' and rules'.
"Information Owner"	Means the natural person within Concentrix organisation which, alone or jointly with others, determines the needs, the objective, purposes and rules of a project including Information processing.
"Intragroup Data Transfer Agreement"	Means the intra-group agreement which comprises the BCR-C and the BCR-P as appendices that all BCR Members are required to execute in order to be bound by the BCR-C and BCR-P
"Information Systems"	Means any Device used directly or indirectly by a User or another Device in order to process Information including, but not limited toc collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Data

"Local Privacy Leader"	Means the person being the main point of contact of the DPO and dealing with data protection matters within each BCR Member.
"Malicious Software"	Means software that by its introduction, adversely affects the intended function of software/hardware. This could include but is not limited to virus, malware, trojans, ransomware etc.
"Networks"	Means the physical or logical connectivity that allows two or more Devices to communicate.
"Password" or "Passphrase"	Means a string of characters or any other logical or physical means used in conjunction with a User Identity during an authentication process to prove identity of a User and/or grand access to certain Information.
"Personal Data"	Means any information relating to an identified or identifiable natural person, (a Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data includes Sensitive Personal Data.
"Personal Data Breach"	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;
"Privacy Committee"	Means the internal board committee supporting the GlobalData Privacy Officer
"Processing" or "Processed"	Means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"Pseudonymisation"	Means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data is not attributed to an identified or identifiable natural person;
"Risk"	Means a scenario describing an event and its consequences, estimated in terms of severity and likelihood.
"Risk management"	Means the coordinated activities to direct and control an organization with regard to risk.

"Security Incident"	Means attempted or successful unauthorised access, use, disclosure, modification, or destruction of Information or interference with system operations in the Information System.
"Sensitive Personal Data"	Means special categories of Personal Data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms requiring such Personal Data to merit specific protection as the context of their Processing could create significant risks to the fundamental rights and freedoms – such as Personal Data that reveals racial or ethnic origin, political opinion, religious or philosophical beliefs, or trade union employees, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sexual orientation.
"Service Agreement"	Means the agreement entered into between a Concentrix affiliate and its Client pursuant to which such Concentrix affiliate provides services to its Client.
"Sub-Processor"	Means the entity engaged by a Data Processor for carrying out specific proces sing activities on behalf of the Data Controller, bound by the same data protection obligations as set out in the contract or other legal act between the Data Controller and the Data Processor
"Software" or "Application"	Means any code, instruction, programs routines that allows directly or remotely the manipulation of Data through any means and includes API, command shells etc.
"Transfer of Personal Data"	Means the Processing, material transfer or distant access to Personal Data from entities established outside of the European Economic Area (EEA).
"User"	Means all Concentrix employees, third parties, third parties' employees, contractors, contractors' employees and other persons whose conduct and duties allows the access to Concentrix Information Systems.
"Concentrix" or "Concentrix Group"	For the BCR and the related Procedures Concentrix shall mean Concentrix SAS and all entities listed in the List of entities bound by the BCR and are therefore BCR Members

17.3 Appendix 05 - Procedure for Data Subjects' requests where BCR Members acts as Data Controller

Table of content

1. Introduction

The adoption of the BCR by the Concentrix group and the commitment from the BCR Members to comply therewith demonstrates BCR Memebrs' commitment to providing a high level of protection to the Personal Data it processes. Concentrix is committed to conducting business in accordance with the Applicable Data Protection Legislation including the European Regulation 2016/679 relating to the processing of Personal Data as of its date of application Concentrix has implemented the following procedure.

The capitalised terms used herein shall have the same meaning as specified under Appendix 2 of the BCR.

2. Objectives of the Procedure

Data Subjects, including employees of BCR Members, are granted specific rights regarding the processing of their Personal Data as further defined under Section 7 of the BCR

When acting as Data Controller, BCR Members shall ensure that any request or complaint from Data Subject in relation to the exercise of their rights ("**Requests**") is addressed in a timely manner as defined hereunder, in order to comply with the BCR and Applicable Data Protection Legislation.

This document describes how BCR Members shall handle a Data Subject's Request where a BCR Member acts as Data Controller (stakeholders, steps and timeline). Where the Request is received from the Data Subjects and that Personal Data is processed by Concentrix BCR Member on behalf of one of Concentrix BCR Members' clients, all requests shall be handled according to the procedure specifically defined under **Appendix 06 - Procedures for handling Data Subjects' requests where Concentrix acts as Data Processor**.

3. Procedures

As a preliminary step, tthe BCRMembers shall expressly inform Data Subjects that they can exercise their rights in accordance with the provisions of Article 7 of he BCR.

3.1 Contact and acknowledgement of receipt of Request

3.1.1 Standard procedure

BCR Members shall also specify how such rights can be exercised. For this purpose, BCR Members will provide Data Subjects with accessible means to exercise their rights and, in particular a single dedicated contact email to be used irrespective of the country a Data Subject is located in. Therefore, any Request as part of this procedure may be sent directly at the following address: dpo@concentrix.com - local emails can be used in order to take into account local specificity, such as language.

On receipt of a Request, the Group Data Privacy Officer ("**DPO**"), or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties, shall ensure they acknowledge receipt thereof no later than 3 working days after the Request was received.

3.1.2 Exception

In the event a complaint from a Data Subject is raised through a different channel than the one described above, the BCR Member or function receiving the complaint shall immediately upon becoming aware, contact the DPO, and (1) internal postal services; (2) Local Privacy Leaders; (3) Business Privacy Referent; and (4) HR departments shall be informed of such procedure.

The Group Data Privacy Officer, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties shall acknowledge receipt of the matter in writing within 2 working days as from the notification by the function.

3.2 Information collection

Prior to transferring a Request internally, the Group Data Privacy Officer, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties, shall (1) ensure that they have obtained the minimum required information from the concerned Data Subject to address his/her Request (2), if deemed necessary, obtain as much information as possible to enable that the Request to be duly handled.

As a minimum, and to the extent possible, it shall obtain the following information ("**Minimum Information**"):

- First and last name of the Data Subject; and
- Where legally permitted/requested, copy of the Data Subject's ID or any other document required as a proof of identity; and
- Contact details to be used for reverting to the Data Subject; and
- The Personal Data concerned by the Request and the subject matter of the latter; and
- Date when Personal Data where initially collected; and
- Type of right that the Data Subject wants to exercise (please indicate whether access, deletion, blocking or correction).

If deemed necessary, BCE Members shall obtain the following information:

- BCR Member which initially collected the Personal Data; and
- Category of processing in relation to which the Data Subject is submitting his/her Request;
- Any relevant details regarding the Request.

In order to obtain the necessary information, the BCR Member can invite the Data Subject, who has not specified sufficient information in their email, to further complete a question form, with free text field, or any other means introduced by Concentrix to facilitate the required information collection from the Data Subject. (e.g. pre-fill form field, options available through checkbox etc.). Means allowing collection of data shall, at a minimum, indicate (1) if the answer is mandatory or not and (2) the consequences if answer is not provided.

3.3 Request assessment

The DPO, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties, shall assess if they have obtained the Minimum Information for handling the Request.

Based on the information requested and obtained, the DPO shall assess the Request. If he/she considers that the Request is reasonable and legitimate (as opposed to a Request with no proof of the Data Subject identity, an excessive demand resulting from repetitive Requests, Request of data already deleted according to the retention period, Requests on behalf of others, career forecast data, etc.) then:

The DPO shall (i) document any Request received and (ii) make the relevant assessment of the Request. In order to properly assess the Request, the DPO, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the hereinabove duties may need to answer to the following questions:

- What is the nature of the Request? (access, deletion, opposition, rectification, portability) ;
- Do I have enough information to identify the Data Subject? ;
- Do I have enough information regarding the scope of the Request? (geographical and material scope) ;
- Does the Data Subject already have possession or easy access to the requested data (e.g., through Concentrix systems)? ;
- Does the Request include information which is not in a clear format for Data Subjects? If yes, make sure you explain the codes so that the information can be understood;
- Is the Data Subject Request based on a legitimate interest? ;
- Is it technically possible to address the Data Subject's Request (given in particular the volume of data at stake)? ;
- Are third parties involved in the processing of Data Subjects' Personal Data within the scope of the Request? ;
- Would the handling of the Request imply that third parties' Personal Data would need to be communicated to the Data Subject? If yes, is it possible to only extract the Personal Data of the requestor, with reasonable efforts and without a risk for the third parties' Personal Data? If no, this Personal Data cannot be communicated to the Data Subject.

3.4 Answer type identification

On this basis, one can contemplate three different cases:

3.4.1 Case 1

Where the information provided by the Data Subject **is not sufficient** to handle the Request, the DPO, or any other individual or entity, internal or external appointed by the DPO for the purpose of managing the following duties, shall send a request for additional information to the Data Subject no later than 10 working days after receiving the Request.

Where the Request is too complex and subject to compliance with any legal requirement, the timeline of the response may be extended up to 2 months, subject to documentation of the assessment of the complexity by the DPO.

3.4.2 Case 2

Where the DPO considers in their initial assessment, that the Request may **not be legitimate as described in section 3.7**, he/she shall not immediately close the case. The Group Data Protection Officer, or any other individual or entity, internal or external, appointed by the DPO for the purpose of managing the following duties shall reply to the Data Subject within 10 working days after receiving the Request, by asking the Data Subject to provide further explanations as to why the Data Subject intends to exercise its rights.

Where necessary, the DPO may inform the relevant stakeholders at local level and the Local Privacy Leader.

Upon receipt of further justification regarding the legitimacy of the Request, the DPO, or the Local Privacy Leader shall, within 15 working days after receiving the information from the Data Subject, (1) make sure that it responds to the Request, or (2) Where he or she considers during the first analysis that the Request addressed by the Data Subject is not legitimate, document why it considers the Request not legitimate and reply to the Data Subject.

Guidance for assessing the legitimacy of the Request is provided above of such procedure. The response shall include the reason for not taking an action and the possibility for the Data Subject to lodge a complaint with a data protection authority and to seek a judicial remedy.

Where the DPO or the relevant privacy network member (i.e., Regional and/or Local Provacy Leader) considers that, based on the additional elements, the Request can be handled it shall ensure that it responds to the Data Subject within the above mentioned 15 working days. Where the Request is too complex and subject to compliance with any legal requirement, the timeline of the response may be extended up to 2 months, subject to documentation of the assessment of the complexity by the DPO.

3.4.3 Case 3

Where information provided by the Data Subject is sufficient, the DPO shall make sure that it responds to the Request without undue delay and maximum **1 month from the receipt of the Request.**

Please note that in any case the response to a data subject must occur within 1 month at the latest after receiving the request (except in certain and limited circumstances as further detailed herein).

3.5 Local mandatory provisions

The Local Privacy Leader, if not directly appointed by the DPO for the purpose of managing the answers to Requests received by a BCR Member, shall be ready to cooperate with the DPO by providing the latter with any relevant information in relation to the matter. The DPO shall then give guidance as to how to handle the case, by taking into account the local circumstances, within 7 working days after receiving the information from the Local Privacy Leader.

3.6 Escalation process

Where the Data Subject is not satisfied with the initial response provided by the Local Privacy Leader or the DPO, and resulting from the handling procedure described above, such Data Subject shall be entitled in any case to immediately ask for his or her Request to be re-examined.

Data Subject shall provide to the BCR Member a detailed explanation of the unsatisfactory provisions of the solution previously provided. DPO shall inform the Privacy Committeel of such request, and allow the Privacy Committee to proceed to the analysis of such request.

Taking into consideration the analysis provided by the Privacy Committee, and without disclosing such analysis to the Data Subject, the DPO, shall take no longer than 2 months from receipt of the Request for re-examination to determine how it shall be handled and shall inform the Data Subject in writing accordingly.

3.7 Refusal of a Request

Although BCR Members are committed to handling Data Subject Requests efficiently, under certain circumstances, BCR Members may be entitled not to accept a Data Subject's Request.

BCR Members are entitled to decline a Data Subject's Request, where accessing the Data Subject's Request would actually or potentially mean that the following information would be shared with the Data Subject:

- **information covered by legal privilege;**
- **information which a BCR Member is legally forbidden to communicate;**
- **information BCR Members are processing during the course of an ongoing investigation or pending litigation procedure.**

Where information/Personal Data regarding other Data Subjects is visible, data may be redacted before it is shared with the Data Subject.

In addition, where a Data Subject objects further processing of his/her Personal Data and/or asks for the deletion of his/her Personal Data, BCR Members may decline such Request where there is a legal obligation on, or an over-riding legitimate interest for a BCR Member to retain the Personal Data. This shall be assessed on a case by case basis and duly documented.

In any case, if a Data Subject Request or complaint is rejected by a BCR Member or the answer does not satisfy the Data Subject, the Data Subject can contact the DPO and / or can directly lodge a complaint with its competent Supervisory Authority.

3.8 Communication with Data Subjects

When communicating with the Data Subject, BCR Members shall cooperate with the Data Subject and address any Request in a timely manner. All communication shall be provided using clear and plain language, in an intelligible, concise, easily accessible and understandable form.

The information to be provided to Data Subjects shall be accurate and limited to (i) what the Data Subject has requested and (ii) the list of information that may be

provided by a Data Controller according to the Applicable Data Protection Legislation.

As a general rule, BCR Members shall not apply fees for reasonable Data Subject Requests. However, under certain circumstances, in particular where the handling of the Request would require significant effort froma BCR Member, reasonable fees, subject to a national maximum according to applicable laws, may apply provided that the Data Subject is informed about such fees in advance.

-

Questions regarding this procedure or knowledge of a violation or potential violation of this procedure must be reported directly to the Group Data Protection Officer.

17.4 Appendix 11-A BCR-C List of Purposes of Processing and related Categories of Personal Data and Data Subjects (Material Scope)

In addition to the provisions of section 2.1 on the material scope of this BCR-C, the table below provides further details on the Transfers performed under this BCR-C. This table details on the Purpose of Processing and the related categories of Data Subjects and Personal data covered by the present BCR-C. The table provided in section 1 below gives details about the transfers of personal data carried out between BCR Members listed in Appendix 1 under this BCR-C.

The countries to which the Personal Data may be transferred depend on the localization of BCR Members involved in the Processing activities and is provided in Appendix 1. Note that as regard BCR-C, Transfers of Personal Data mostly occur between the BCR Members of a same Region (except for the Global entities where there may be transfers between such Global entities and all other BCR Members depending on the Purposes of Processing. For more transparency, we have included an additional table presenting the Regions in section 2 of the present Appendix.

1. Table on Transfers of Personal Data between BCR Members listed in Appendix 1 under this BCR-C

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
HR processing activities	**Recruitment management**	**1.Identification data** (e.g., Name, Last name. E-Mail, Phone number, picture (if provided), Address) **2. Economic and financial data** (e.g., salary expectation) **3. Professional data** (e.g., CV-resume Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and	**Candidates**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		copy of their work permit (only if necessary)) **4. Background check** (results of background check (only the results, and for successful candidates to be hired)	
	Employee records management (incl. Onboarding process, maintenance of employee record in accordance with the applicable legislation, administrative follow-up of occupational medicine, internal directory)	**1.Identification data** (e.g., Name, Last name, E-Mail, Phone number, picture of the data subject, Address, Gender, family status) **2.Professional data** (e.g., CV-Resume , Educational records and information regarding skills of the employee, Previous experience, Diplomas/certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary), Employee internal identification number, office location, previous work history, Business Unit Division Line Reporting Manager, contract type) **3.Economic and financial data** (e.g., Income/Salary, IBAN/BIC) **4. Sensitive data** (social security number)	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Payroll Management	**1.Identification data** (e.g., Name, Last name, E-Mail, Phone number, Address) **2. Professional data** (e.g., Employee internal identification number, contract type, hours of work) **3. Economic and financial data** (e.g., Payment data (worked hours, absences, compensation and benefits, bonus, Benefits and Entitlements Data), salary wage, IBAN/BIC) **4.Sensitive data** (Social Security number)	**BCR Members' employees**
	Referral Program management	**1. Identification data** (e.g., Name, Last name, E-Mail, Phone number, Address). **2. Professional data** (e.g., CV-resume Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings).	**BCR Members' employees Candidates**
	Badge management for employees	**1.Identification data** (e.g., Name, last name, phone number) **2.Professional data** (e.g., job title role, Employee internal identification number), Employee badge number, authorized areas and working hours)	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		3.Economic and financial data (e.g., payment attached to the use of the canteen)	
	Employee's training management (incl. Internal training and client's training)	**1.Identification data** (e.g., Name, Last name, E-Mail, Phone number, Address) **2.Professional data** (e.g., Job title role, Employee internal identification number, Training information (type of training, date, attendance, quiz results, etc.), office location, previous work history Business Unit Division, line Reporting Manager)	**BCR Members' employees**
	Employee's career and mobility management	**1.Identification data** (e.g., Name, Last name . E-Mail, Phone number, picture (if provided), Address) **2. Professional data** (e.g., CV-resume, Current job title role, Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary))	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Employees' background check	**1.Identification data** (e.g., Name, Last name. E-Mail, Phone number, photo (if provided), Address) **2. Professional data** (e.g., CV-resume, Current job title role, Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary)) **4. Background check information** (e.g., background check results)	**BCR Members' employees**
	Employees' absence and working time management	**1. Identification data** (e.g., Name, Last name) **2. Professional data** (e.g., Employee internal identification number, office location, previous work history, Business Unit Division Line Reporting Manager, contract type, hours of work, work schedule, absences (sick leaves, vacations, etc.))	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Professional elections management	**1.Identification data** (e.g., Name, Last name, age) **2. Professional data** (e.g., Preparation of the electoral list (identity of voters, age, seniority, college), applications management (identity, nature of the mandate applied for, information allowing to verify compliance with eligibility requirements, if applicable trade-union membership declared by the candidates) and release of the results of the elections (identity of the candidates, mandates concerned, number and percentage of votes obtained, identity of the elected employees and, if applicable, trade-union membership of the elected employees).	**BCR Members' employees**
	Management of Employees representative bodies' committees	**1. Identification data** (e.g., Name, Last name) **2. Professional data** (e.g., Convocations, preparatory documents, reports, various minutes of representative bodies' committee).	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Employees' performance and evaluation management	**1. Identification data** (e.g., Name, Last name). **2. Professional data** (e.g., information on evaluation: dates of the evaluation interviews, identity of the evaluator, professional competencies of the employee, objectives assigned, results objectives, results obtained, assessment of professional skills on the basis of objective criteria with a direct and necessary link to the job, observations and wishes formulated by the employee, career development forecasts. For agents, transcription of call conversation with end customer may be used for quality assessment purposes).	**BCR Members' employees**
	Quality assessment of agents / operators	**1. Identification data** (e.g., Name, Last name, email) **2. Professional data** (e.g., Employee internal identification number, job title role, Line reporting managers, KPIs, objectives assigned, results objectives, results obtained, assessment of professional skills on the basis of objective criteria with a direct and necessary link to the job, observations and wishes formulated by the	**BCR Members' agents/operators**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		employee, career development forecasts. transcription of call conversation with end customer may be used for quality assessment purposes, evaluation results)	
	Employee Wellbeing Program	**1. Identification data** (e.g., Name, Last name, email) **2. Professional data** (e.g., internal ID number, survey score, care conversation scheduled, job position, line manager, shifts, working hours, quality assessment results, etc.)	**BCR Members' employees (moderators)**
	Impact sourcing program management (recruitment, reporting, etc.)	**1.Identification data** (e.g., Name, Last name . E-Mail, Phone number, photo (if provided), Address) **2. Economic and financial data** (e.g., salary expectation) **3. Professional data** (e.g., CV-resume Previous experience, Diplomas, certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary), source of recruitment)	**Candidates, BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Travel and expenses management	**1. Identification data** (e.g., Name, Last name, Address) **2. Professional data** (e.g., Job title role, employee internal identification number, booking reservation, dates of travel, business justification, line reporting manager) **3. Economic and financial data** (e.g., expenses report, invoices, IBAN / BIC)	**BCR Members' employees**
	Social & cultural activities management	**1. Identification data** (e.g., Name, Last name, Address, marital status/relationship) **2. Professional data** (e.g., Job title role, employee internal identification number) **3. Economic and financial data** (e.g., income, benefits and benefits claimed and provided)	**BCR Members' employees (and their declared relatives)**
Company life & services	**IT Management (IT equipment allocation and management, service desk)**	**1. Identification data** (e.g., Name, Last name email address) **2. Professional data** (e.g., employee internal identification number, job title role, office location, line reporting manager, IT request information (Ticket number, request topic, request follow-up) **3 Technical and connection data** (e.g., IP Address, user account	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		information, Device ID, , necessary professional applications and websites)	
	Internal Information Security (Fraud Prevention)	**1. Identification data** (e.g., Name, Last name email address) **2. Professional data** (e.g., employee internal identification number, job title role, office location, line reporting manager) **3 Technical and connection data** (e.g., IP Address, user account information, Device ID, alter, results of alerts)	**BCR Members' Employees**
	CCTV within Concentrix facilities	**1.Identification data** (e.g. footages)	**BCR Members' employees** **Visitors to BCR Members' premises**
	Management of telephony in the workplace	**1. Identification data:** (e.g. name, last name, email address, phone number) **2.Technical and connection data** (e.g., IP Address, Logins, Device ID data, type of phone, relevant information regarding the use of telephony services and data necessary for invoicing purposes, including	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		operator, the nature of the call (local, national, international), the duration of the call, the time and date of the beginning and end of the phone call and the invoice)	
	Internal communication to Employees (incl., internal communication by email, or via Virtual private networks (intranet))	**1.Identification data** (e.g., Name, Last name email address). **2.Professional data** (e.g., charts, discussion areas, information areas applications and networks) **.4.Technical and connection data** (e.g., IP Address, Device ID data, user account information)	**BCR Members' employees**
	Employees Survey and form	**1.Identification data** (e.g., Name, Last name email address, phone number) **2.Technical and connection data** (e.g., employee internal identification number, job title role, office location, anonymous & aggregated results)	**BCR Members' employees**
	Internal Directory & Employees' user access and accounts management	**1.Identification data** (e.g., Name, Last name email address). **2.Professional data** (e.g., charts, discussion areas, information areas applications and networks).	**BCR Members' employees**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		3. Technical and connection data (e.g., IP Address, Device ID data, user account information)	
	Internet access and control and prevention of data loss	**1.Identification data** (e.g., Name, Last name email address) **2.Professional data** (e.g., employee internal identification number, job title role, office location, line reporting manager, authorized application & website, employee job title role) **.4.Technical and connection data** (e.g., IP Address, Device ID data, user account information)	**BCR Members' employees**
Legal / Compliance	**Fraud Prevention and detection**	**1. Identification data** (e.g., Name, Last name, email, phone number). **2. Technical and connection data** (e.g.,IP Address, Logins ,Device ID data, interaction data, bug reports, monitoring information embedded in the application, device used). **3. Interaction data necessary to investigate a potential fraud** (e.g., Identification through the means used to provide the services and contact the End Customers; Voice data of the End Client	**BCR Members' employees** **BCR Members customers/clients**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		and the Service Provider's employee, transcription of the interaction. Telephone number, email address, operations planning, operations performance indicators and peer performance indicators)	
	Whistleblowing system	**1.Identification data** (e.g., name last name, email, phone number, details of the people author of the alert, of the people subject of the alert and of people involved in the processing of the alert) **2. Professional data** (e.g., contract type, job title role, Function/job of the person(s) reporting the incident, the person(s) implicated in the incident and the person(s) involved in the investigation**)** **3. Information of the alert** (e.g., facts reported, evidence as part of the investigation, record of investigations follow-up of the alert).	**BCR Members' employees and administrators**
	Corporate & Legal entities management *(incl. Mandates and proxy, Delegation of powers and signatures, Corporate reporting (boards,*	**1.Identification data** (e.g., Name or company name, E-Mail , Phone number) **2.Professional data** (e.g., (e.g., CV-Resume , Educational records and information regarding skills of the employee,	**BCR Members' employees and administrators**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	committees), Professional associations, external counsels directory)	Previous experience, Diplomas/certificates, foreign languages spoken, assessment of knowledge and trainings, number and copy of their work permit (only if necessary), Employee internal identification number, office location, delegation of authorities, proxy) **3.Economic and financial data** (e.g., Payment ,Income/Salary, Financial situation ,invoices, Credit card n umber ,IBAN / BIC)	
	Employees' litigation and disciplinary procedures	**1.Identification data** (e.g., Name, Last name, E-Mail, Phone number, footage (if necessary), Address) **2. Professional data** (e.g., employee internal identification number, office location, line reporting manager, information related to potential disciplinary actions and procedure for employees, nature of litigation for business related litigation, job title role / function) **Information related to the litigation matter** (e.g., subject matter, estimated risks, evidence, etc.)	**BCR Members' employees** **Attorneys**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Litigation management	**1.Identification data** (e.g., Name, Last name, E-Mail , Phone number, footage (if necessary), Address) **2. Professional data** (e.g., nature of litigation for business related litigation, job title role / function) Information related to the litigation matter (e.g., subject matter, estimated risks, evidence, etc.)	**BCR Members' employees** **BCR Members' business partners** **Attorneys**
	Clients and business partners database (BtoB)	**1.Identification data** (e.g., Name or company name, E-Mail, Phone number, Address Of headquarters) **2. Professional data** (e.g., job title role) **3.Economic and financial data** (e.g., Payment ,Income/Salary, Financial situation, invoices, Credit card number ,IBAN / BIC)	**BCR Members' Business partners/ Clients**
Operation & Marketing	**Client and prospect leads management**	**1.Identification data** (Name, Last name, E-Mail, Phone number, professional Address) **2.Professional data** (job title, role, company name, office location) **3. Economic and financial data** (client agreement, invoice, dunning, purchase orders).	**BCR Members' Clients/Prospects (business contact)**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Concentrix Direct marketing campaigns	**1.Identification data** (Name, Last name, E-Mai, Phone number, professional Address) **2.Professional data** (job title, role, company name, office location, optout decision)	**BCR Members' Clients/Prospects (business contact)**
	Processing of Payment Services - WPS	**1.Identification data** (e.g. Name, Last name ,ID card, E-Mail , Phone number, Postal Address , Gender, internal references) **2.Professional data** (e.g., Information related to the profession, information related to the regulatory qualification of a politically exposed person) **3. Economic and financial data** (e.g. Payment, Income/Salary, Financial situation, invoices, IBAN / BIC)	**BCR Members' Clients/Prospects**
Partner/Vendor relationships	**Suppliers Management and Contract Management**	**1.Identification data** (e.g.,Name , E-Mail , Phone number, Address Of headquarters) **2.Professional data** (e.g., Job titles, copy of supplier agreements, invoice, dunning, purchase orders)	**BCR Members' employess** **Supplier's Business contact**

Domain of Processing activities	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
	Data broker relationship management	**1.Identification data** (e.g., Name, E-Mail, Phone number, address) **2. Professional data** (e.g., Job title role, line reporting manager, optin/optout, hobbies, contractual relationship, invoice, dunning)	**BCR Members' employees** **Data broker's Business contact Webhelp Client/Prospect (business contact)**

2. Table on BCR Members' Regions

Concentrix Geo/Regions	Countries included in the Geo/ Region
Group (Global)	**All countries*** **Transfers may occur between Global entities (including Global Shared Services entities) and all other BCR Members entities of the Group, whatever their country of location identified in Appendix 1*

AMERICAS	**Canada** **Colombia** **El Salvador** **Guatemala** **Honduras** **Mexico** **Nicaragua** **Peru** **US**
APAC	**Australia** **China** **Hong Kong** **Japan** **Malaysia** **Philippines** **Singapore** **Thailand**
CRIT	**Albania** **Czech Republic** **Italy** **Slovakia**
DACH	**Austria** **Bosnia-Herzegovina** **Bulgaria** **Germany** **Hungary** **Kosovo** **North Macedonia** **Poland** **Slovenia** **Switzerland**

FRANCE	**Algeria** **Benin** **France** **Greece** **Ivory Coast** **Madagascar** **Morocco** **Portugal** **Romania** **Senegal**
MET	**Egypt** **Israel** **Jordan** **Saudi Arabia** **Turkey**
NETHERLANDS	**The Netherlands** **Surinam**
NORDICS	**Denmark** **Estonia** **Finland** **Latvia** **Lithuania** **Norway** **Sweden**
SPAIN	**Spain**
UK	**India** **Sout Africa** **United Kingdom**

WPS/WKS	**Belgium** **France** **Germany** **Italy** **Portugal** **Spain** **United Kingdom** **United States** *Transfers may occur between WPS/WKS affiliates only.*
NETINO	**France** **Madagascar**
WEBHELP MEDICA	**France** **Portugal** **Spain** *Transfers may occur between Webhelp Medica affiliates only.*

DOCUMENT CONTROL

Version	Update	Modification summary
0.1	27/02/2022	Final approval
0.2	01/01/2023	Update of list of BCR Members
0.3	24/02/2023	Update of list of BCR Members
0.4	01/04/2024	Re-branding and formatting Alignment with EDPB Recommendations 1/2022 repealing and replacing WP256_Rev01
0.5	10/12/2024	Appendix 01 Update of list of BCR Members (change of names and liquidated entities) Update of Webhelp SAS name to Concentrix SAS in the core of the BCR
0.6	04/08/2025	Appendix 01 Update of list of BCR Members (change of names and liquidated entities)

Review Frequency	This document will be reviewed at least annually or upon significant change(s)
Date of Issue	25/05/2018
Domain	Privacy
Classification	Public
Reference	Binding Corporate Rules - Controller