Collibra's Binding Corporate Rules: Processor Policy

Table of Contents

PART I: INTRODUCTION TO THIS PROCESSOR POLICY

Collibra's Binding Corporate Rules: Processor Policy ("BCR" or "the Policy") establishes Collibra's ("we" "our", "us") approach to compliance with EU data protection laws when processing personal data on behalf of a third party controller.

Members of our group of companies that are bound by this Policy are listed in Appendix 1 ("Group members").

1. Scope of these BCR

The standards described in the BCR are worldwide standards that apply to all Group members when processing any personal data as a processor under this Policy. Accordingly, these BCR apply regardless of the geographic origin of the personal data that we process, the country in which we process personal data, or the country in which a Group member is established.

These BCR apply when we process personal data as a processor on behalf of a third party controller located in the EU/EEA, including when the personal data is transferred to a Group member for processing outside of the EU/EEA. These BCR apply regardless of whether our Group members process personal data by manual or automated means.

For an explanation of some of the terms used in these BCR, like "controller", "process", and "personal data", please see the section titled "Important terms used in these BCR" below.

2. *Types of personal data within the scope of these BCR*

These BCR apply to all personal data that we process as a processor on behalf of a third party controller (referred to as the "Customer" in these BCR), including personal data processed in the course of providing services to a Customer or another Group member – such as:

- Authorised user data: contact information and roles or titles of end users of Customers of Collibra's Services;
- Source Data: raw data elements comprising data sets, or samples thereof, that Customers submit to Collibra's Services to profile, sample, classify, catalogue or otherwise determine characteristics of such data sets; and

- Platform data: data or content that classifies, organizes, defines or otherwise characterizes Source Data or Customer's enterprise data structure (i.e., metadata) which establishes within Collibra's Services comprehensive data catalogues, data governance structures, business glossaries, business process descriptions, data stewardship roles and responsibilities, asset and domain lists and similar data governance concepts. Platform data also includes logs, insights, statistics, or reports that Collibra generates regarding the performance, availability, usage, integrity or security of the Service.

When a Customer transfers personal data to us for processing in accordance with these BCR, a copy of these BCR shall be incorporated into the contract with that Customer.

3. Our collective responsibility to comply with these BCR

All Group members and their staff must comply with these BCR when processing personal data as a processor on behalf of a Customer, irrespective of the country in which they or the Customer are located. All Group members have entered into a legally binding and enforceable intra-group agreement which requires them to comply with these BCR. If a Group member breaches a provision of the intra-group agreement, any Group member, including Collibra Belgium BV, can bring an enforcement action against the member in breach.

In particular, all Group members who process personal data as a processor under this Policy must comply with:

- the rules set out in Part II of these BCR;
- the practical commitments set out in Part III of these BCR;
- the third party beneficiary rights set out in Part IV; and
- the related policies and procedures appended in Part V of these BCR.

4. Responsibility towards the Customer

As a data processor, Collibra has a number of direct legal obligations under EU data protection laws. In addition, Customers assign certain data protection obligations to Collibra in their contracts appointing Collibra as their processor. Such contracts shall meet the requirements of Article 28 of the GDPR. If Collibra fails to comply with the terms of its processor appointment, it may put the Customer in breach of EU data protection laws and Customer may initiate proceedings against Collibra for breach of contract.

A Customer may enforce these BCR against any Group member that is in breach of its contractual obligations owed to the Customer. Where a non-EU/EEA Group member (or a non-EU/EEA external sub-processor appointed by a Group member) processes personal data for which a Customer is a controller in breach of these BCR, that Customer may enforce the BCR against Collibra Belgium BV. In such event, Collibra Belgium BV will be responsible for demonstrating that such Group member (or external sub-processor) is not responsible for the breach, or that no such breach took place.

When a Customer transfers personal data to a Group member for processing in accordance with these BCR, these BCR are made binding towards such customers in the contract with that Customer. If a Customer chooses not to rely on these BCR when transferring personal data to a Group member outside of the EU/EEA, that Customer is responsible for implementing other appropriate safeguards in accordance with EU data protection laws.

5. Management commitment and consequences of non-compliance

Collibra's management is committed to ensuring that all Group members and their staff comply with these BCR at all times. These BCR ensure that our Customers can trust Collibra to process their personal data appropriately, fairly and lawfully, no matter where such personal data may be processed within the Collibra organization.

Further, non-compliance with these BCR may result in sanctions for Collibra from competent data protection authorities and courts, and may cause harm or distress to individuals whose personal data has not been protected in accordance with the standards described in these BCR.

In recognition of the importance of trust to Collibra's business and the gravity of the risks associated with violating that trust, staff members who do not comply with these BCR will be subject to disciplinary action, up to and including dismissal.

6. Access to these BCR

These BCR are accessible on Collibra's website at Public Version - Collibra - BCR (Processor)(04.05.2023)(123283128.1).

7. Important terms used in these BCR

For the purposes of these BCR:

- the term "EU data protection laws" refers to the EU's General Data Protection Regulation (EU) 2016/679 of the EU Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;
- the term "controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- the term "Customer" refers to the third party controller on whose behalf Collibra processes personal data. It includes Collibra's third party Customers, as well as Collibra Group members, when we process personal data on their behalf in the course of providing data processing services to them.
- the term "data protection authority(ies)" means the applicable EU/EEA independent public authority(ies) that is responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data.
- the term "EEA" refers to the European Economic Area.
- the term "EU" refers to the European Union.
- the term "Group member" means the members of Collibra's group of companies listed in Appendix 1;
- the term "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- the term "processing" 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. The term "process" and "processed" shall be construed accordingly.
- the term "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. For example, Collibra is a processor of personal data that Customers submit to Collibra's software-as-a-service platform and Collibra processes this data on behalf of its Customers;
- the term "BCR" refers to this Binding Corporate Rules: Processor Policy. The BCR apply where Collibra processes personal data as a processor on behalf of a Customer;
- the term "special categories of personal data" means information that relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data

concerning health, or data concerning a natural person's sex life or sexual orientation. For the purpose of these BCR, it also includes information about an individual's criminal offences or convictions, as well as any other information deemed sensitive under EU data protection laws; and

- the term “staff" refers to all employees, new hires, former employees, individual contractors and consultants, and temporary staff engaged by any Collibra Group member. All employees must comply with these BCR.

8. How to raise questions or concerns

If you have any questions regarding these BCR, your rights under these BCR or EU data protection laws, or any other data protection issues, you can contact Collibra’s Privacy team using the details below. Collibra’s Privacy team will either deal with the matter directly or forward it to the appropriate person or department within Collibra to respond.

Attention:	Privacy team

Email:	privacy@collibra.com
Address:	Collibra Belgium BV (VAT BE 0899.079.439) Picardstraat 11 B 205, Picardstraat 11 B 205, 1000 Brussels – BELGIUM Attention: Data Protection Officer Attention: Data Protection Officer

Collibra’s Privacy team is responsible for ensuring Group members and Customers whose personal data is processed by Collibra are notified of changes to this Policy.

If you want to exercise any of your data protection rights, please email your request to privacy@collibra.com. Alternatively, if you are unhappy about the way in which Collibra has used your personal data, you can raise a complaint in accordance with our complaint handling procedure set out in Appendix 3.

PART II: OUR OBLIGATIONS

These BCR apply where a Group member processes personal data as a processor anywhere in the world. All staff and Group members must comply with the following obligations:

Rule 1 – Lawfulness:

- *We* must *ensure that processing is at all times compliant with applicable law and these BCR.*
- *We must at all times comply with any EU data protection laws, as well as the standards set out in these BCR, when processing personal data.*

Accordingly:

- where EU data protection laws exceed the standards set out in these BCR, we must comply with those laws; but
- where EU data protection laws do not meet the standards set out in these BCR, we must process personal data in accordance with the standards set out in these BCR.

Rule 2 – Cooperation with Customers:

- We must cooperate with and assist the Customer to comply with its obligations under EU data protection laws in a reasonable time and to the extent reasonably possible.

We must cooperate with and assist our Customers to comply with their obligations under EU data protection laws. We must provide this assistance within a reasonable time and as required under the terms of our contract with the Customer. Assistance may include, for example, helping our Customer keep the personal data we process on its behalf accurate and up-to-date, or helping our Customer to provide individuals with access to their personal data, or helping our Customer to conduct data protection impact assessments in accordance with EU data protection laws.

Rule 3 – Fairness and Transparency:

- We must, to the extent reasonably possible, assist the Customer to comply with the requirement to explain to individuals how their personal data will be processed.

Our Customer has a duty to explain to the individuals whose data the Customer processes (or instructs us to process), how and why that data will be used. This information must be given in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

We will provide assistance and information to the Customer in accordance with the terms of our contract with the Customer as required to assist them in complying with this requirement. This is usually done by means of an easily accessible fair description of processing within our published Data Processing Addendum.

Rule 4 – Processing Limitation:

- *Where we are acting as a processor, we will only process personal data on behalf of, and in accordance with the instructions of, the Customer.*

Where we process personal data as a processor, we must only process that personal data on behalf of the Customer and in accordance with its documented instructions (for example, as set out in the terms of our contract with the Customer), including with regard to any international transfers of personal data.

If we are unable to comply with our Customer's instructions (or any of our obligations under these BCR), we will inform the Customer promptly. The Customer may then suspend its transfer of personal data to us and/or terminate its contract with us (in accordance with the terms of the contract).

In such circumstances, we will return, anonymize, destroy or store the personal data, including any copies of the personal data, in a secure manner or as otherwise required, in accordance with the terms of our contract with the Customer and, if requested, certify to the Customer that this has been done.

If legislation prevents us from returning the personal data to our Customer, or from destroying it, we must inform the Customer. In such an event, we must continue to maintain the confidentiality of the personal data and not actively process the personal data further other than as required by such legislation and in accordance with the terms of our contract with the Customer.

Rule 5 – Data Accuracy and Minimization:

- *We will assist our Customer to keep the personal data accurate and up to date.*

We must assist our Customer with complying with its obligation to keep personal data accurate and up-to-date. In particular, where a Customer informs us that personal data is inaccurate, we must assist our Customer to update, correct or erase that data without undue delay.

We must also take measures to inform Group members or external sub-processors to whom the personal data has been disclosed of the need to update, correct or erase that personal data.

Rule 6 – Storage Limitation:

- *We will assist our Customers to store personal data only for as long as is necessary for the purpose for which the information was initially collected.*

Where a Customer instructs us that personal data we process on its behalf is no longer needed for the purposes for which it was collected, we will assist, either through self-service tools or otherwise, our Customer to erase or anonymize that personal data without undue delay and in accordance with the terms of our contract with the Customer. We must also take measures to inform Group members or external sub-processors to whom the personal data has been disclosed of the need to erase or anonymize that personal data.

Rule 7 – Security, Integrity and Confidentiality:

- *We must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk to the personal data we process on behalf of a Customer.*

Where we provide a service to a Customer which involves the processing of personal data, the contract between us and that Customer will set out the technical and organizational security measures we must implement to safeguard that data consistent with EU data protection laws. We must ensure that any staff member who has access to personal data processed on behalf of a Customer does so only for purposes that are consistent with the Customer's instructions and is subject to a duty of confidence.

Rule 8 – Personal Data Breach Reporting:

- *We must notify a Customer of any personal data breach that we experience if it presents a risk to the personal data we process on the Customer's behalf.*

When we become aware of a personal data breach that presents a risk to the personal data that we process on behalf of a Customer, we must immediately inform the Privacy team and follow our personal data breach

management policies.

The Privacy team will review the nature and seriousness of the personal data breach and determine whether it is necessary to notify a Customer. The Privacy team shall be responsible for ensuring that any such notifications, where necessary, are made without undue delay and in accordance with applicable law.

We will, taking into account the nature of processing and information available to Collibra, assist a Customer with any obligations that Customer may have to notify such a personal data breach to competent data protection authorities and data subjects.

Rule 9 – Engaging Sub-processors:

- *We may only appoint, add or replace sub-processors with authorization from the Customer and in accordance with its requirements.*

We must obtain a Customer's authorization before appointing, adding or replacing a sub-processor to process personal data on its behalf. Authorization must be obtained in accordance with the terms of our contract with the Customer.

We must make available to our Customer up-to-date information about the sub-processors we intend to appoint in order to obtain its authorization. If, on reviewing this information, a Customer objects to the appointment of a sub-processor in the manner described in the Customer's contract, Collibra and the Customer will make a good faith attempt to resolve the issues. If no resolution is reached, the Customer will have the right to terminate the contract.

Rule 10 – Sub-processor Contracts:

- *We must only appoint sub-processors who protect personal data to a standard that is consistent with these BCR and our contractual terms with Customers. We will impose the data protection obligations as set out in Article 28 of the GDPR and these BCR on our sub- processors, and, in particular, provide sufficient guarantees to implement appropriate technical and organizational measures. Where our sub-processors fail to fulfil their data protection obligations, we shall remain fully liable to our Customers for the performance of our sub-processors' obligations.*

We must only use internal sub-processors (i.e., Group members) or appoint external sub-processors who provide sufficient guarantees in respect of the commitments made by us in these BCR. In particular, sub-processors must implement appropriate technical and organizational security measures to protect the personal data they process, and such measures must be the same as our commitments to our Customer under our contractual terms with the Customer.

Where we intend to appoint an external sub-processor to process personal data, we must undertake due diligence to ensure it has in place appropriate technical and organizational security measures to protect the personal data. We must impose strict contractual obligations in writing on all sub-processors that require them to comply with these BCR's obligations, our contractual data protection obligations with our Customers, and the data protection obligations in Article 28 of the GDPR, including to:

- These BCR;
- Process personal data only on behalf of and under Collibra's instructions; Notify Collibra of all personal data breaches and security incidents and directly notify impacted Customers if requested by Collibra;
- Implement and maintain appropriate technical and organizational measures, having regard to the state of the art and the cost of their implementation, to protect personal data against unauthorized access or disclosure, including by way of a comprehensive written information security program. These measures should ensure a

level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected and should be consistent with standards contained in these BCR (and in particular Rules 7 and 8 above);

- Inform Collibra if it cannot comply with its data protection obligations or when it receives requests from Individuals or from a public authority;
- Only transfer personal data outside of the EU/EEA in compliance with Articles 45, 46 and 47 of the GDPR (as described below);
- Only sub-contract the processing of personal data with Collibra's prior written consent or after informing Collibra pursuant to the terms of Collibra's general written authorization and under an agreement that imposes on the sub-processor the same data protection obligations as set out in the contract between the Customer and Collibra;
- Ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Assist Collibra in ensuring compliance with its obligations pertaining to the security of the personal data, data protection impact assessments and related prior consultations;
- At the choice of Collibra, delete or return the personal data to the Group Members after the end of the provision of the services;
- Make available to Collibra information necessary to demonstrate compliance with its obligations under the agreement and inform Collibra if, in its opinion, an instruction infringes EU Data Protection Law; and
- Remain liable to the Customer and/or Collibra for the performance of its obligations.

In relation to transfers to external sub-processors outside the EU/EEA and established in countries not ensuring an adequate level of protection, the member of the Collibra Group that undertakes to enter into an agreement with the sub-processor, ensuring that adequate protection is provided in accordance with the EU/EEA rules on cross border data flows, e.g. the EU Standard Contractual Clauses adopted by the EU Commission 2021/914/EU, and, where the appropriate safeguards contained in the agreement cannot be effectively complied with due to the law and/or the practices in the recipient's country – in particular due to possible access to the personal data by public authorities of the recipient's country - adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU/EEA standard of essential equivalence. The agreement shall ensure, that the sub-processor must comply with the same obligations as the member itself according to the service agreement with the data controller and these BCRs. If no sufficient supplementary measures can be put in place, the member of the Collibra Group must suspend the transfer immediately, and, if the transfer does already take place, demand that the sub-processor return all personal data processed on behalf of the Collibra Group member and delete existing copies. The outcome of any evaluations carried out as described in this section and any proposed supplementary measures will be documented and made available to the relevant supervisory authorities on request.

Rule 11 – Respect for Individuals' Data Protection Rights:

- *We must assist our Customer to comply with its duty to respect the data protection rights of individuals, in accordance with the instructions of our Customer and the terms of our contract with the Customer.*
- *We will assist a Customer to respond to queries or requests made by individuals in connection with their personal data.*

In particular, if any Group member receives a request from any individual wishing to exercise his or her data protection rights in respect of personal data for which the Customer is the controller, the Group member must transfer such request promptly to the relevant Customer and not respond to such a request unless authorized to do so by the Customer or required by law.

Rule 12 - Privacy By Design and By Default

- *We must provide our products and services in a way that assists our Customer to apply privacy by design and by default principles.*

We must provide our products and services in a way that assists our Customer to implement privacy by design and privacy by default principles. This means that we must implement appropriate technical and organizational measures when providing our products and services that:

- are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards in order to protect the rights of individuals and meet the requirements of EU data protection laws ("privacy by design"); and
- ensure that, by default, only personal data which are necessary for each specific processing purpose are collected, stored, processed and are accessible; in particular, that by default personal data is not made accessible to an indefinite number of people without the individual's intervention ("privacy by default").

These measures must be implemented in accordance with the terms of our agreement with our Customer.

PART III: DELIVERING COMPLIANCE IN PRACTICE

To ensure we follow the rules set out in our BCR, in particular the obligations in Part II, Collibra and all of its Group members must also comply with the following practical commitments:

1. *Resourcing and compliance: We must have appropriate staff and support to ensure and oversee privacy compliance throughout the business.*

   Collibra has appointed its Privacy team to oversee and ensure compliance with these BCR. The Privacy team is responsible for overseeing and enabling compliance with these BCR on a day-to-day basis.

   As part of the Privacy team, Collibra's Data Protection Officer ("DPO") is responsible for providing advice, guidance and training on the implementation of, and compliance with, all applicable privacy laws, along with governance and monitoring of, and reporting regarding internal policies and procedures within Collibra. The DPO shall also provide advice and guidance to facilitate compliance with all of Collibra's policies throughout any change management process. The DPO will enjoy the highest management support in exercising their function and will report directly to Collibra's General Counsel.

   The DPO will be supported by Privacy Liaisons from the following corporate departments: Marketing, People, Legal Product, Engineering, Finance, Sales, Customer Success and Information Security. Each Privacy Liaison represents a department, or subset of a department, and each is responsible for identifying core personal data processing functions within his / her department or subset thereof. Privacy Liaisons are responsible for maintaining their department (or sub-department's) portion of Collibra's records of processing of personal data. The Privacy Liaisons must meet quarterly with the DPO to discuss key privacy issues arising within the field or within Collibra specifically, ask privacy related questions, and discuss obligations related to the processing

of personal data. Privacy Liaisons are responsible for sharing any new information learned applicable to the processing of personal data within their respective departments/sub-departments to their respective departments/sub-departments. They are also responsible for receiving and responding to or escalating employee reports of privacy non-compliance.

2. *Privacy training: We must ensure staff are educated about the need to protect personal data in accordance with these BCR.*

   Group members must provide appropriate privacy training to staff members who:

   - have permanent or regular access to personal data; or
   - are involved in the processing of personal data or in the development of products, services or tools used to process personal data.

   We will provide such training in accordance with the Privacy Training Program (see Appendix 2).

3. *Records of Data Processing: We must maintain records of the data processing activities carried out on behalf of a Customer.*

   We must maintain a record of the processing activities that we conduct on behalf of a Customer in accordance with EU data protection laws. In accordance with Article 30(2) of the GDPR, these records must contain the following elements:

   - the name and contact details of the relevant Group member and Customer on behalf of which the Group member is acting, and, where applicable, their representatives and data protection officers;
   - the categories of processing carried out on behalf of each Customer;
   - where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and
   - where possible, a general description of the technical and organisational security measures.

   These records should be kept in writing (including in electronic form) and we must make these records available to competent data protection authorities upon request. The Privacy team is responsible for ensuring that such records are maintained.

4. *Audit: We must have data protection audits on regular basis.*

   We will have data protection audits to ensure verification of compliance with all aspects of these BCR on an annual basis, including methods of ensuring that corrective actions will take place. Such audits may be conducted by either internal or external auditors. In addition, we will conduct data protection audits on specific request from the Data Protection Officer, General Counsel or the Audit Committee of the Board of Directors (“Audit Committee”).

   We will communicate the results of these audits to Collibra’s Data Protection Officer, General Counsel and where appropriate, either Collibra’s Chief Executive Officer or the Audit Committee.

5. *Complaint handling: We must enable individuals to raise data protection complaints and concerns.*

   Group members must enable individuals to raise data protection complaints and concerns (including complaints about processing under these BCR) by complying with the Complaint Handling Procedure (see Appendix 3).

6. *Cooperation with competent data protection authorities: We must always cooperate with competent data protection authorities.*

   Group members must cooperate with competent data protection authorities by complying with the Cooperation Procedure (see Appendix 4).

7. *Updates to these BCR: We will update these BCR in accordance with our Updating Procedure.*

   Whenever updating our BCR, we must comply with the Updating Procedure.

8. *Conflicts between these BCR and national legislation: We must take care where local laws conflict with these BCR, and act responsibly to ensure a high standard of protection for the personal data in such circumstances.*

   No Group Member has any reason to believe that local laws and practices applicable to the processing of the personal data by that Group Member, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Group Member from fulfilling its obligations under these BCR. This 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 objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these BCR.

   In reaching this conclusion, the Group Member has taken due account in particular of the following elements:

   - the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   - the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
   - any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these BCR, including measures applied during transmission and to the processing of the personal data in the country of destination.

   The Group Member will make its best efforts to provide the transferring Customer with relevant information in relation to this assessment and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these BCR.

   The Group Member will document, with the transferring Customer, this assessment and make it available to the competent supervisory authorities on request.

   The Group Member will notify the transferring Customer promptly if, after having agreed to these BCR and for the duration of the contract with that transferring Customer, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under this paragraph 8, including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in this paragraph 8.

   Following such a notification, or if the transferring Customer otherwise has reason to believe that the Group Member can no longer fulfil its obligations under these BCR, the transferring Customer or transferring Group Member shall promptly identify appropriate measures (e.g. technical or

organisational measures to ensure security and confidentiality) to be adopted by the Customer and/or Group Member to address the situation. The transferring Customer shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authorities to do so. In this case, the transferring Customer shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these BCR. If the contract involves more than two parties, the transferring Customer may exercise this right to termination only with respect to the relevant party, unless the parties have agreed otherwise.

9. *Government requests for disclosure of personal data: We must comply with the Government Data Request Procedure in respect of a legally binding request for disclosure of personal data.*

   If a Group member receives a legally binding request from a law enforcement authority or state security body for disclosure of personal data which is processed on behalf of an EU/EEA Customer under these BCR, it must:

   - notify the EU/EEA Customer promptly unless prohibited from doing so by a law enforcement authority or applicable law; and
   - use its best efforts to put the request on hold and notify the appropriate data protection authority competent for the EU/EEA Customer and the appropriate data protection authority competent for Collibra as processor by complying with the requirements of its Government Data Request Procedure.

   In no event must transfers of personal data from a Group member to any law enforcement, state security or similar public authority be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

PART IV: Third Party Beneficiary Rights

1. Application of this Part IV

This Part IV applies where individuals' personal data are protected under EU data protection laws. This is the case when:

- those individuals' personal data are processed in the context of the activities of a Customer (acting as controller) or a Group member (acting as processor) established in the EU/EEA;
- a non-EU/EEA Customer (acting as controller) or Group member (acting as processor) offers goods and services (including free goods and services) to those individuals in EU/EEA; or
- a non-EU/EEA Customer (acting as controller) or Group member (acting as processor) monitors the behavior of those individuals, as far as their behavior takes place in the EU/EEA;

and that Customer or any Group member (as applicable, and whether or not that Group Member is itself established in the EU/EEA) then transfers those individuals' personal data to a non-EU/EEA Group member (or its external sub-processor) for processing under the BCR.

2. Entitlement to effective remedies

When this Part IV applies, individuals have the right to pursue effective remedies in the event their personal data is processed by Collibra in breach of the following provisions of these BCR:

- Paragraph 6 (Access to these BCR) under Part I;

- Part II (Our Obligations) of;
- Paragraphs 5 (Complaints Handling), 6 (Cooperation with Competent Data Protection Authorities), 8 (Conflicts between these BCR and national legislation) and 9 (Government requests for disclosure of personal data) under Part III of;
- Part IV (Third Party Beneficiary Rights) of;
- Appendix 3 (Complaints Handling Procedure);
- Appendix 4 (Cooperation Procedure); and

3. Individuals' third party beneficiary rights

When this Part IV applies, the right for individuals to pursue effective remedies against Collibra under these BCR applies only if either:

a. the obligation at stake has been specifically imposed on Collibra in accordance with the GDPR or a data processing agreement implementing the GDPR, in particular the duty to:

- respect the instructions received from the Customer;
- implement appropriate technical and organizational security measures;
- notify any personal data breach to the Customer;
- respect the conditions to engage an external sub-processor;
- cooperate with and assist the Customer in complying and demonstrating compliance with the law;
- provide easy access to BCRs;
- grant a right to complain through an internal complaint mechanism;
- cooperate with the DPA; and
- respect requirements pertaining to liability, compensation and jurisdiction and conflicts of law EU/EEA-, or

b. the individuals cannot bring a claim against a Customer because the Customer has factually disappeared or ceased to exist in law or has become insolvent and no successor entity has assumed the entire legal obligations of the Customer by contract or by operation of law.

In such cases, individuals may exercise the following rights under these BCR:

- *Complaints*: Individuals may complain to a Group member and/or to an EU data protection authority, in accordance with the Complaints Handling Procedure at Appendix 3;
- *Proceedings*: Individuals may commence proceedings against a Group member for violations of these BCR, in accordance with the Complaints Handling Procedure at Appendix 3;
- *Compensation*: Individuals who have suffered material or non-material damage as a result of an infringement of these BCR have the right to receive compensation directly from Collibra or any third party involved in the same processing for the entire damage suffered.
- *Transparency*: Individuals also have the right to obtain a copy of the BCR on request to the Privacy team at privacy@collibra.com.

4. Responsibility for breaches by non-EU/EEA Group members

Collibra Belgium BV will be responsible for ensuring that any action necessary is taken to remedy any breach of the BCR by a non-EU/EEA Group member (or a non-EU/EEA external sub-processor appointed by a Group member).

In particular:

- If an individual can demonstrate damage it has suffered likely occurred because of a breach of these BCR by a non-EU/EEA Group member (or a non-EU/EEA external sub-processor appointed by a Group member), Collibra Belgium BV will have the burden of proof to show that the non-EU/EEA Group member (or non-EU/EEA external sub-processor) is not responsible for the breach, or that no such breach took place.
- where a non-EU/EEA Group member (or a non-EU/EEA external sub-processor appointed by a Group member) fails to comply with these BCR, individuals may exercise their rights and remedies above against Collibra Belgium BV and, where appropriate, receive compensation (as determined by a competent court or other competent authority) from Collibra Belgium BV for any material or non-material damage suffered as a result of a breach of these BCR.

PART V: RELATED POLICIES AND PROCEDURES

Appendix 1

COLLIBRA GROUP MEMBERS

Part A: Collibra Group members in the EU/EEA

	Name of entity	**Registered address**	**Registration numbers**
1.	Collibra B.V.	Laarderhoogtweg 25 1101EB Amsterdam — NETHERLANDS	87719606
2.	Collibra Belgium BV	Picardstraat 11 B 205, 1000 Brussels – BELGIUM	0792 250 864
3.	Collibra Czech s.r.o.	Klimentska 1216/46, Nove Mesto, 110 00 Prague 1, CZECH REPUBLIC	243 14 307

4.	CNV Belgium (Collibra France)	Spaces La Défense, Le Belvédère, 1-7 cours Valmy, Puteaux, Paris 92800 – FRANCE	922 014 329
5.	Collibra Polska Sp. z o.o.	Ul. Św. Antoniego 2/4, brama A, 50-073 Wrocław – POLAND	0000471698
6.	Collibra España S.L.	Avenida de Bruselas 15, 2ª Planta, 28108 Alcobendas Madrid — SPAIN	B42930107
7.	Collibra Netherlands B.V.	Laarderhoogtweg 25, 1101EB Amsterdam – NETHERLANDS	862228773
8.	Collibra Sweden filial	Time Advokatbyrå, Biblioteksgatan 11, Box 590, 114 11 Stockholm – SWEDEN	516411 6690
9.	CNV Data Intelligence GmbH (Collibra Germany)	Regus Business Center FÜNF HÖFE, Theatinerstraße 11, 80333 München - GERMANY	HRB 268641

Part B. Collibra Group members outside of the EU/EEA

	Name of entity	**Registered address**	**Registration Number**
1.	Collibra AU Pty Ltd	152 Elizabeth St Suite 08-115, Melbourne - AUSTRALIA	627439294
2.	Collibra Inc.	61 Broadway, 31st Floor, New York, NY 10006 – UNITED STATES OF AMERICA	5299941
3.	Collibra Public Sector LLC	c/o Corporation Trust Company, 1209 Orange Street, Wilmington, DE 19801 – UNITED STATES	5918812
4.	Collibra UK Limited	120 Moorgate, London, EC2M 6UR – UNITED KINGDOM	09637739
5.	Collibra Canada Ltd.	44 Chimpan Hill Suite 1000, Saint John NB E2L 2A9 - CANADA	718010

Appendix 2

PRIVACY TRAINING PROGRAM

1. Background

1.1 The BCR provide a framework for the transfer of personal data between Collibra's Group members ("Group members") and sets out the requirements for Collibra to train its staff members on the requirements of the Policy.

1.2 All staff must be trained to understand general privacy and data security principles, with an emphasis on compliance with the GDPR, at least once annually. The training is conducted and monitored for completion by the Information Security and the People teams.

1.3 In addition, the DPO's quarterly meetings with the Privacy Liaisons serve as training sessions on key privacy topics relevant to Collibra. Privacy Liaisons are expected to disseminate their learnings to their respective departments (and sub-departments).

1.4 These trainings are further described below.

2. Training on data protection

Collibra's training on data protection and the BCR covers the following main areas:

1. GDPR Overview
    a. What is GDPR
    b. Risk Minimization
    c. Data Management Under GDPR
    d. Organizational Impact
    e. Penalties for Noncompliance

2. GDPR in Action
    a. Company Responsibilities
    b. Privacy by Design
    c. Individual Rights
    d. Data Storage & Security
    e. Data Breach Notification

3. PII Fundamentals
    a. Identifying, Classifying and Protecting PII
    b. Determining Risk Level of PII
    c. Implementing PII Safeguards

3. Training on information security

Collibra's training on information security and security certifications applicable to Collibra (e.g., ISO 27001) covers the following main areas:

1) Security Essentials
2) Social Engineering
3) Introduction to Phishing

4) Insider Threat Overview
5) Password Policy
6) Safer Web Browsing

Appendix 3

COMPLAINT HANDLING PROCEDURE

1. Background

Collibra's BCR safeguard personal data transferred between the Collibra Group members ("Group members").

This Complaint Handling Procedure describes how complaints brought by an individual whose personal data is processed by Collibra under the BCR must be addressed and resolved without undue delay and in any event within one month, extendable to two months if so required by the complexity and number of requests received, in which case the individual will be informed accordingly within the first month following receipt by Collibra of the complaint.

This procedure will be made available to Customers on whose behalf Collibra processes personal data under the BCR.

2. *How individuals can bring complaints*

Subject to Part IV (Third Party Beneficiary Rights), any individuals may raise a data protection question, concern or complaint (whether related to the Policy or not) by e-mailing Collibra's Privacy team at privacy@collibra.com or by writing to Collibra's DPO at:

Attn. Data Protection Officer
Collibra, BV
Picardstraat 11 B 205,
1000 Brussels – BELGIUM

3. Complaints process

3.1. *Communicating complaints to the Customer*

3.1.1. Where a complaint is brought in respect of the processing of personal data for which Collibra is a processor on behalf of a Customer, Collibra will communicate the details of the complaint to the relevant Customer without delay and without handling it (unless Collibra has agreed in the terms of its contract with the Customer to handle complaints).

3.1.2. Collibra will cooperate with the Customer to investigate the complaint, in accordance with the terms of its contract with the Customer and if so instructed by the Customer.

3.2 What happens if a Customer no longer exists?

3.2.1. In circumstances where a Customer has disappeared, no longer exists or has become insolvent, and no successor entity has taken its place, individuals whose personal data are processed under the BCR have the right to complain to Collibra and Collibra will handle such complaints in accordance with paragraph 3 of this Complaint Handling Procedure.

3.2.2. In such cases, individuals also have the right to complain to a competent data protection authority and to file a claim with a court of competent jurisdiction, including where they are not satisfied with the way in which their complaint has been resolved by Collibra. Such complaints

and proceedings will be handled in accordance with paragraph 4 of this Complaint Handling Procedure.

4. Right to complain to a competent data protection authority and to commence proceedings

4.1 Overview

4.1.1. Where individuals' personal data:

a. are processed in the EU/EEA by a Group member acting as a controller and/or transferred to a Group member located outside the EU/EEA; or
b. are processed in the EU/EEA by a Group member acting as a processor and/or transferred to a Group member located outside the EU/EEA under the BCR;
c. then those individuals have certain additional rights to pursue effective remedies for their complaints, as described below.

4.1.2. The individuals described in paragraph 4.1.1. have the right to complain to a competent data protection authority (in accordance with paragraph 4.2) and/or to commence proceedings in a court of competent jurisdiction (in accordance with paragraph 4.3), whether or not they have first complained directly to the Customer in question or to Collibra.

4.1.3. Collibra acknowledges that complaints and claims made pursuant to paragraphs 4.2 and 4.3 may be lodged by a not-for-profit body, organization or association acting on behalf of the individuals concerned.

4.2 Complaint to a data protection authority

4.2.1. If such an individual wishes to complain about Collibra's processing of his or her personal data to a data protection authority on the basis that an EU/EEA Group member has processed personal data in breach of the Policy or in breach of EU data protection laws, he or she may complain about that EU/EEA Group member to the data protection authority in the EU/EEA territory:

a. of his or her habitual residence;
b. of his or her place of work; or
c. where the alleged infringement occurred.

4.2.2. If an individual wishes to complain about Collibra's processing of his or her personal data to a data protection authority on the basis that a non-EU/EEA Group member has processed personal data in breach of the Policy or in breach of EU data protection laws, then Collibra Belgium BV will submit to the jurisdiction of the competent data protection authority (determined in accordance with paragraph 4.2.1 above) in place of that non- EU/EEA Group member, as if the alleged breach had been caused by Collibra Belgium BV.

4.3 Proceedings before a national court

4.3.1. If an individual wishes to commence court proceedings against Collibra on the basis that an EU/EEA Group member has processed personal data in breach of the Policy or in breach of EU data protection laws, then he or she may commence proceedings against that EU/EEA Group member in the EU territory:

a. In which that EU/EEA Group member is established; or
b. of his or her habitual residence.

4.3.2. If an individual wishes to commence court proceedings against Collibra on the basis that a non-EU/EEA Group member has processed personal data in breach of the Policy or in breach of EU data protection laws, then Collibra Belgium BV will submit to the jurisdiction of the competent national court (determined in accordance with paragraph 4.3.1 above) in place of that non-EU/EEA Group member, as if the alleged breach had been caused by Collibra Belgium BV.

Appendix 4

COOPERATION PROCEDURE

1. Introduction

1.1. This Cooperation Procedure sets out the way in which Collibra will cooperate with competent data protection authorities in relation to the BCR.

2. Cooperation Procedure

2.1. Where required, Collibra will make the necessary personnel available for dialogue with a competent data protection authority in relation to the BCR.

2.2. Collibra will review, consider and (as appropriate) implement:

a. any advice or decisions of relevant competent data protection authorities on any data protection law issues that may affect the BCR; and
b. any guidance published by data protection authorities (including the European Data Protection Board or any successor to it) in connection with Binding Corporate Rules for Processors.

2.3. Subject to applicable law and respect for the confidentiality of the information provided, Collibra will provide upon request copies of the results of any audit Collibra conducts of the BCR to a competent data protection authority.

2.4. Collibra agrees that:

a. a competent data protection authority may audit any Group member located within its jurisdiction for compliance with the Policy, in accordance with the EU data protection law(s) of that jurisdiction; and
b. a competent data protection authority may audit any Group member who processes personal data for a Customer established within the jurisdiction of that data protection authority for compliance with the Policy, in accordance with the EU data protection law(s) of that jurisdiction;

with full respect to the confidentiality of the information obtained.

2.5. Collibra will cooperate with requests, queries or complaints from competent data protection authorities. Collibra will follow the recommendations of the Belgian data protection authority and other competent data protection authorities regarding the implementation of the BCR.