CONTROLLER BINDING CORPORATE RULES

I. INTRODUCTION

As a global leader in enterprise cloud data management, Informatica LLC, Informatica Ireland EMEA UC, and the subsidiaries listed in Appendix A (together the "**Informatica Group**") is committed to honoring individuals' rights to respect for private and family life and to the protection of personal data. This commitment is embraced throughout the Informatica Group, from our boards of directors to each employee, and is reflected in the way we design and configure our products and services and the way we conduct our business. These Controller Binding Corporate Rules ("**BCR**"), by addressing measures to provide adequate protection for the transfer and processing of personal data by the Informatica Group as a data controller of personal data relating to its employees and business contacts, together with the verification by the Informatica Group on a regular basis of such supplementary measures as may reasonably be required, examples of which are outlined at Appendix G, are an important part of that commitment. These BCR will be available and easily accessible to business contacts on the Informatica Group's external website at https://www.informatica.com/legal.html, as well as being available to employees on the Informatica Group intranet.

All entities that comprise the Informatica Group, and all employees of such entities, are required to comply with the BCR.

These BCR were developed to satisfy the standards set forth in the European Union General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"). They will be available on the Informatica Group's external website at https://www.informatica.com/legal.html.

II. DEFINITIONS

Terms in these BCR will be interpreted consistent with the GDPR. The following terms used commonly throughout the BCR will have the following meanings:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject') who is either an employee or business contact; 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.
>
> '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, organization, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"competent supervisory authority" is the public authority responsible for supervising the application of GDPR in the relevant European Union member state.

‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or Member State law.

'data exporter' means a controller (or, where permitted, a processor) established in the European Union that transfers personal data to a data importer.

'data importer' means a controller or processor located in a jurisdiction outside of the European Economic Area that receives personal data from a data exporter.

'data protection' for the purpose of these BCR means the protection of personal data in accordance with the provisions of the GDPR, including as to how such data is collected, processed and / or transferred.

‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

‘employee’ means current employees of the Informatica Group, and, where applicable, prospective employees who have submitted an application for employment to the Informatica Group, as well as former employees and dependents of an employee.

‘business contact’ means an individual who has, or who works on behalf of a party that has, a direct business relationship with the Informatica Group, including customers, vendors, suppliers and partners and who the Informatica Group can identify, directly or indirectly, based on the personal data Informatica Group collects about that individual in the context of that relationship.

“special categories of personal data” means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

III. SCOPE

A. Organizational Scope

The BCR bind and apply to all processing of personal data by, and all transfers of personal data among, the entities comprising the Informatica Group. A complete list of entities comprising the Informatica Group and the jurisdictions in which they are established is provided in Appendix A.

B. Geographic Scope

The BCR apply to all transfers and processing of personal data by and among the Informatica Group worldwide.

C. Substantive Scope

The BCR apply to the transfer and processing of all personal data of prospective, current, and former employees ("**Employee Data**") and all personal data of business contacts ("**Business Contact Data**"). The categories and the purpose of processing of Employee Data and Business Contact Data are listed in Appendix F.

Employee Data may include special categories of personal data relating to health, trade union membership, and racial or ethnic origin of employees ("**Special Category Data**"), where processing of such data arises in the context of the employment relationship and in accordance with applicable EU and EU Member State data protection law ("**Applicable Law**").

Informatica Group entities transfer and process Employee Data for the purposes of managing and administering its work force (*e.g.*, considering candidates, and hiring, paying, providing benefits to, evaluating the performance of, promoting, demoting or disciplining, changing the role of, and terminating employees and maintaining associated employment records), and may rely on third-party service providers to process Employee Data in support of one or more of these purposes (*e.g.*, payroll service or health and other insurance or benefits).

Informatica Group entities transfer and process Business Contact Data for the purposes of promoting, advertising, selling, fulfilling purchases of, responding to questions regarding, and providing technical support regarding its products and services; managing business relationships with business contacts; and complying with legal obligations. For further information, please consult the Informatica Group's Privacy Policy.

The Informatica Group complies with separate processor BCR when transferring or processing personal data provided to the Informatica Group by its customers.

IV. DATA PROTECTION PRINCIPLES

As set forth in greater detail in Section V, Data Protection Safeguards, the Informatica Group complies with the following data protection principles, set forth in the GDPR, when transferring or processing Employee Data or Business Contact Data:

> ***Lawfulness, fairness, and transparency*** -- personal data shall be processed lawfully, fairly and in a manner that is transparent to the data subject;
>
> ***Purpose Limitation*** -- personal data shall be collected for specified, explicit and legitimate purposes and processed only in a manner that is compatible with those purposes;
>
> ***Data Minimization*** -- 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, and personal data identified as inaccurate shall be erased or rectified without 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 are processed; and,

Integrity and confidentiality -- personal data shall be protected using appropriate technical or organizational measures against unauthorized or unlawful processing and against accidental loss, destruction or damage.

V. DATA PROTECTION SAFEGUARDS

A. Lawfulness

The Informatica Group processes Employee Data and Business Contact Data only consistent with laws applicable to the relevant member the Informatica Group, including with the consent of the employee or business contact; for the performance of the employment or business contact contract; where necessary to comply with a legal obligation; and/or where the processing is necessary for the purposes of the Informatica Group's legitimate interests and those interests are not overridden by the interests, rights, or freedoms of the employee or business contact.

To the extent that applicable local data protection laws require a higher level of protection, the Informatica Group provides the level of protection required by applicable local laws. If an Informatica Group member determines that a legal requirement in a non-EU country is likely to prevent it from complying with these BCR or to have a substantive adverse effect on its compliance with these BCR then that member will report the issue promptly to Informatica Ireland EMEA UC and the relevant designated data protection representative (unless prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). The Informatica Group will also report the issue to the competent supervisory authority, including information about the data requested, the requesting body and the legal basis for the disclosure. If the legal requirement involves direct access or a valid legally binding request for the disclosure of personal data by a public authority, including law enforcement or national security authority, the Informatica Group member will promptly notify and keep informed the relevant designated data protection representative, who will in turn promptly notify it to Informatica Ireland EMEA UC and the Global Head of Privacy. In so doing, the Informatica Group member will provide information about the personal data requested, the requesting authority, the legal basis for the request and the response provided. The Informatica Group member acting as importer will document all relevant information with respect to the legal requirement, including any legal advice received from counsel within that jurisdiction on the legal requirement, and will provide the minimum amount of information that is permissible when responding to the legal requirement, such as a request for disclosure, based on its reasonable interpretation of the request.

The Informatica Group member will challenge and / or appeal a decision relating to a legally binding request for information if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. The Informatica Group member shall not disclose

personal data pursuant to a legal requirement, until it is required to do so under the applicable local law. The Informatica Group member will document its legal assessment and any challenge to a legal requirement involving a request for disclosure and, to the extent permissible under the destination country's laws, make the documentation available to Informatica Ireland EMEA UC, and the relevant data protection representative. It shall also make this information available to the competent supervisory authority upon request.

If the legal requirement involves a legally binding request for the disclosure of personal data by a law enforcement or national security authority and the Informatica Group member is prohibited from reporting to Informatica Ireland EMEA UC and to the competent supervisory authority, it shall use best efforts (taking into account the reasonable prospects of success) to obtain a waiver of the prohibition in order to promptly communicate to the competent supervisory authority as much information as it can as soon as possible and document such efforts.

If the member cannot obtain a waiver despite such best efforts, it will preserve the information (meaning all relevant details of the personal data requested, the requesting authority, the legal basis for the request and the response provided) and it will annually provide all relevant information relating to the request and waiver to the competent supervisory authority. The Informatica Group member will seek to make disclosures to law enforcement or national security authorities specific, proportionate, and consistent with what is appropriate in a democratic society. Transfers of personal data to public authorities cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

B. Transparency & Fairness

The Informatica Group will explain to employees and business contacts how it processes their personal data. In particular, the Informatica Group provides employees and business contacts with notice of its data processing practices and all information required by Articles 13 and 14 of the GDPR through these BCR, privacy policies, and other fair processing notices made readily available to employees and business contacts (i) at the time when the personal data are directly obtained, (ii) within a reasonable period, but at latest within one month where the personal data are indirectly obtained, having regard to the specific circumstances in which the personal data are processed, (iii) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject, or (iv) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed. The Informatica Group also provides relevant data subjects such information on their third party beneficiary rights with regard to the processing of their personal data, the means to exercise those rights, relevant liability provisions, and the data protection principles through these BCR, including this Section V and Section VI. Such notice includes: (a) the identity and contact details of the controller; (b) the contact details of the chief privacy officer or data protection officer; (c) the purpose and legal basis for the processing; (d) the legitimate interest pursued by the controller, where relevant; (e) the recipients or categories of recipients of the data; (f) the categories of personal data concerned; (g) information regarding international transfers, including as to the valid legal mechanism relied upon for such transfers; (h) information regarding the retention of the data; (i) information regarding the data subject's rights with respect to the data, as provided for in Article 13(2) of the GDPR; (j) whether the data is used as a basis for automated decision-making and / or profiling, and meaningful information about the logic involved, as well as the significance and the envisaged

consequences of such processing for the data subject; (k) information regarding whether the provision of personal data is a requirement or an obligation on the data subject and of the possible consequences of failure to provide such data; (l) where the origin of the personal data can be provided, the original source of the personal data and, if applicable, whether it came from publicly accessible sources; (m) where the origin of the personal data cannot be provided, general information regarding the source(s).

Where applicable, the Informatica Group also provides employees and business contacts with information regarding international data transfer and sub-processing activities.

The Informatica Group also responds to inquiries or complaints submitted by employees or business contacts regarding the Informatica Group's processing of their personal data through the Complaint Handling Standards.

For further information, please consult the Informatica Group's Privacy Policy for business contacts and Personnel Privacy Notice for employees.

C. Purpose Limitation

The Informatica Group only collects Employee Data and Business Contact Data for specified, explicit, and legitimate purposes and does not process such data in a manner that is incompatible with those purposes. The Informatica Group will only process Employee Data and Business Contact Data if and to the extent permissible under Article 6 and Article 9 of the GDPR. If the Informatica Group intends materially changing the purposes for which it processes Employee Data or Business Contact Data, the Informatica Group will make employees or business contacts aware in advance of the change and seek consent as appropriate.

D. Data Minimization & Accuracy

The Informatica Group collects and processes only that Employee Data and Business Contact Data relevant to the lawful purpose for which it processes such data. The Informatica Group maintains such data which is, to the best of the Group's knowledge, accurate and, where necessary, kept up to date. The Informatica Group shall take every reasonable step to ensure that such data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay. The Informatica Group also responds timely to requests from employees and business contacts to access, update, correct, delete, or anonymize their data, to the extent required by Applicable Law, and communicates regarding such update, correction, deletion, or anonymization to each entity to which the Informatica Group has disclosed Employee Data or Business Contact Data.

E. Storage Limitation

The Informatica Group stores Employee Data and Business Contact Data in accordance with the Group Record Management Policy. The Informatica Group stores such data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Following the conclusion or termination of the processing, the Informatica Group deletes all such data unless Applicable Law requires that the Informatica Group continue to store such data. The Informatica Group informs the employee or business contact of

requirements for continued storage through the Informatica Group's Privacy Policy and Personnel Privacy Notice, maintains the confidentiality of the data, and ceases active processing (including any sub-processing) of the data.

F. Processing of Special Categories of Personal Data

The Informatica Group processes Special Category Data only to the extent necessary for the purposes of carrying out obligations and exercising specific rights in the field of employment (including benefits) or social security and social protection law, assessment of capacity to work, where necessary for the establishment, exercise or defence of legal claims, or with the explicit consent of the relevant employee. Access to Special Category Data is restricted to recruiting and HR personnel, and IT support personnel for HR and recruiting systems, on a need to know basis.

G. Data Protection by Design & by Default

The Informatica Group has established appropriate technical and organizational measures and integrated safeguards into its processing to implement the data protection principles in an effective manner and to protect the rights and freedoms of data subjects ("**data protection by design**"). The Informatica Group has also implemented appropriate technical and organizational measures for ensuring that only personal data which are necessary for a specific, legitimate purpose are processed and that any default settings or parameters are designed with data protection in mind ("**data protection by default**").

H. Integrity & Confidentiality

The Informatica Group processes Employee Data and Business Contact Data in a manner designed to ensure that it is appropriately secured. In particular, the Informatica Group implements appropriate organizational, physical, and technical measures to protect against unauthorized or unlawful processing and against accidental loss, destruction, or damage. Such measures include, as appropriate, pseudonymization and encryption of such data. Such measures are designed to meet the requirements of Applicable Law.

In the event of unauthorized or unlawful processing, or accidental loss, destruction, or damage, of Employee Data or Business Contact Data, the Informatica Group will, without undue delay, and, where feasible, not later than 72 hours after becoming aware of such an incident, document the incident (and provide applicable documentation to the relevant supervisory authority on request) and notify (i) Informatica Ireland, and the relevant supervisory authorities (unless unlikely to result in a risk to the rights and freedoms of natural persons); (ii) the relevant designated data protection representative (who shall act in accordance with Section VII.D below); and (iii) the relevant employee or business contact (where likely to result in a high risk to their rights and freedoms).

I. Data Subject Rights

The Informatica Group maintains appropriate technical and organizational measures to honor and fulfill employee and business contact requests regarding their rights as data subjects. Where appropriate, the Informatica Group will assist employees and business contacts in exercising their rights, including:

- **The right of access –** the right to receive a copy of their personal data processed by by the Informatica Group, subject to certain exemptions such as the protection of the rights and freedoms of third parties (and a reasonable fee may be applicable for such access requests by a data subject);

- **The right to rectification –** the right to correct or supplement personal data if that data is incomplete or incorrect;

- **The right to erasure –** the right to have the personal data erased where the data subject's consent has been withdrawn or the applicable lawful basis for processing no longer applies;

- **The right to restriction of processing –** the right to restrict the processing of personal data where the data subject has: made an objection to the processing (see *The right to object* below); contested the accuracy of the data; where the processing is unlawful; or where the data subject requires the data for the purpose of a legal claim;

- **The right to data portability –** where processing of the personal data is carried out by automated means and on the basis of the data subject's consent or a contract, data subjects may be entitled to obtain their personal data in a format that makes it easier to re-use the information in another context, and to transmit this data to another data controller without hindrance;

- **The right to object –** the right to object to certain types of processing of your personal data where the processing is carried out in connection with tasks in the public interest, under official authority or in the legitimate interests of others; and

- **The right not to be subject to a decision based solely on automated processing (including profiling) which produces legal or similarly significant effects concerning the employee or business contact**.

The Informatica Group also maintains a process for responding to inquiries and complaints by employees and business contacts regarding the processing of their personal data. This includes the implementation of a centralised email account (privacy@informatica.com) for data subject requests. Any data subject request received via an alternative means will be re-directed by the relevant Informatica employee to the centralised email account without undue delay.

On receipt, each request will be logged and triaged by a dedicated Informatica team that consists of legal counsel trained to respond to data subject rights requests. Requests may be referred by this response team to supervisory privacy counsel at Informatica for assistance and review in appropriate cases. Informatica will inform the relevant data subject of any such extension within one month.

Informatica will issue an interim response to any requests received to indicate that the request is being processed, and will respond to requests within 1 month of receipt of a valid request, except in limited circumstances where an extension (of up to two months) is permitted pursuant to applicable data protection legislation, taking into account the complexity and number of the requests.

Complaints in relation to the Informatica Group's handling of any data subject rights will be handled in accordance with Section VII.B below.

J. Onward Transfer & Processors

The Informatica Group may transfer onward data only where, having assessed the law and practices in the third country of destination applicable to the processing, including any legal requirements to disclose personal data or measures authorising access by public authorities, it concludes it is not prevented 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 GDPR, are not in contradiction with the BCR.

In undertaking an assessment, account will be taken of the specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same third country or to another third country, including:

- purposes for which the data are transferred and processed;
- types of entities involved in the processing;
- economic sector in which the transfer or set of transfers occur;
- categories and format of personal data transferred;
- location of the processing including storage; and
- transmission channels used.

The Informatica Group will document appropriately such assessment as well as relevant contractual, technical or organisational safeguards to be put in place to supplement the safeguards under the BCR, examples of which are outlined at Appendix G, and shall make such documentation available to the competent supervisory authority on request.

The relevant Informatica Group controller includes the required contractual language from Article 28 of the GDPR in its contracts with processors of Employee Data or Business Contact Data, including with processors within or external to the Informatica Group. These contracts obligate processors to process the personal data only on documented instructions from the relevant Informatica Group controller, including with regard to transfers of personal data to a third country or an international organization. Any onward transfer of Employee Data or Business Contact Data to a processor, whether a member of or outside of the Informatica Group will be pursuant to an appropriate data transfer mechanism where required by these BCR, including standard contractual clauses approved by the European Commission.

Through a combination of diligence and contractual obligations, Informatica Group has taken steps to bind its processors to the same level of protection as provided in these BCR. Informatica

Group's processors located in the EEA are bound by and must comply with EEA data protection law, which provides the same level of protection as these BCR. Informatica Group also has taken steps to impose requirements by contract that are consistent with the requirements of Applicable Law and these BCR. Where required by these BCR, the Informatica Group will ensure each such contract includes requirements to:

- process the personal data only on documented instructions from an Informatica Group member, including with regard to transfers of personal data to a third country or an international organisation;

- ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- take reasonable technical and organizational measures and other measures required under these BCR to secure the data;

- obtain prior written approval from Informatica Group before engaging any sub-processor, and ensure that the sub-processor is subject to the contractual obligations which are no less protective than those contained in the Informatica processor agreement;

- assist Informatica Group in fulfilling its obligations to respond to requests for exercising the data subject's rights under these BCR;

- assist Informatica Group in ensuring compliance with all other obligations of Informatica Group under these BCR, including security requirements, data breach notification, conducting data protection impact assessments and consulting with the relevant supervisory authorities;

- delete or return all the personal data to Informatica Group after the end of the provision of services relating to processing, at the choice of Informatica Group; and

- make available to Informatica Group all information necessary to demonstrate compliance with the obligations in the contract and allow for and contribute to audits, including inspections, conducted by Informatica Group or another auditor mandated by Informatica Group (collectively, the "**Contract Requirements**").

If Informatica Group desires to use a processor located in a country outside of the EEA which is not subject to an adequacy decision to process EU personal data it will do so pursuant to standard contractual clauses, adopted by the European Commission, and implement supplementary measures as necessary, examples of which are outlined at Appendix G.

K. Accountability

In addition to the safeguards outlined in this Section V and in Sections VII.A and VII.C below, the Informatica Group maintains written records of its processing activities that meet the requirements of Article 30 of the GDPR. These records shall contain the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

- the purposes of the processing;

- a description of the categories of data subjects and of the categories of personal data;

- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

- 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) of the GDPR, the documentation of suitable safeguards;

- where possible, the envisaged time limits for erasure of the different categories of data; and

- where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR.

The Informatica Group, prior to processing, also carries out data protection impact assessments for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons in accordance with Article 35 of the GDPR. Where a data protection impact assessment is conducted, which indicates that the processing would result in a high risk in the absence of measures to mitigate the risk, the Informatica Group will consult the competent supervisory authority, prior to processing in accordance with Article 36 of the GDPR.

Informatica Group members acting as data exporter in an EU Member State shall monitor, on an ongoing basis, and where appropriate in collaboration with data importers, developments in the third countries to which data has been transferred that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

VI. THE BINDING NATURE OF THE BCR

A. Informatica Group Members, Employees

All members of the Informatica Group, and all employees of any such member, respect and comply with the BCR. These BCR are legally binding upon Informatica Group members and employees.

B. Employee & Business Contacts

i. Data Subject Third Party Beneficiary Rights

These BCR recognize the right of employees and business contacts, to enforce these BCR as third-party beneficiaries, where their personal data is processed by the Informatica Group pursuant to these BCR. A relevant employee or business contact, whose personal data is processed by the Informatica Group, may enforce these BCR as a third party beneficiary.

As part of that enforcement, those data subjects may lodge a complaint with a data protection authority or court against the EU member of the Informatica Group responsible for such violation or against Informatica Ireland EMEA UC, the EU headquarters and designated EU entity with delegated responsibilities for the BCR. Relevant data subjects may (or pursuant to Article 80 of GDPR via a not-for-profit body, organization or association) bring their claims either before the supervisory authority in the Member State in which they work, the Member State in which they reside, or the Member State in which the alleged infringement occurred; or before the competent court of the Member State in which Informatica Group or its processors have an establishment, or before the competent court of the Member State in which the data subject resides.

The relevant data subjects have a right as third-party beneficiaries to enforce against the Informatica Group compliance with:

- Section V, Data Protection Safeguards;
- Section VI.B, Binding Nature of the BCR;
- Section VII.B, Complaint Handling; and,
- Section VIII, Duty to Cooperate with Data Protection Authorities

ii. Allocation of Responsibility within the Informatica Group

An employee or business contact, where their personal data is processed by the Informatica Group pursuant to these BCR, may enforce the above provisions of these BCR against any member of the Informatica Group that violates the BCR, and in the event that a member responsible for a violation of these BCR is outside the EU, against Informatica Ireland EMEA UC, the EU headquarters and designated EU entity with delegated responsibilities for the BCR.

If an Informatica Group member outside the EU violates the BCR, the courts or other competent authorities in the EU, will have jurisdiction and the relevant data subject will have the rights and remedies against Informatica Ireland EMEA UC as if the violation had taken place by Informatica Ireland EMEA UC in Ireland.

The Informatica Group member or Informatica Ireland EMEA UC shall have the burden of proof to demonstrate that it is not liable for damage suffered by a relevant data subject as a result of the violation of the Sections set forth above. If a violation of the Sections set forth above is established, the Informatica Group will agree to take the necessary action to correct or remedy the violation and be liable for any appropriate sanction and any material or non-material damage suffered by the relevant data subject as a result of the violation.

VII. COMPLIANCE WITH THE BCR

A. Employee Compliance, Training & Awareness Raising

Informatica Group has developed a comprehensive set of policies and standards that implement the BCR throughout Informatica Group. Informatica Group's policies and standards require compliance by all Group employees and provide for disciplinary measures in the event of non-compliance up to and including termination of employment.

The Informatica Group provides appropriate and up-to-date training to relevant personnel on the requirements of these BCR and Applicable Law, both on onboarding and no less frequently than annually. Role-specific training modules are included within Informatica's online training, and supplemental, role-specific training on an ad hoc basis is provided for personnel that have permanent or regular access to personal data, who are involved in the collection of personal data or in the development of tools used to process personal data.

The Informatica Group also makes its internal data protection policies and procedures available to all employees on its company intranet. The general counsel or designated officer with primary responsibility for data protection communicates with the Informatica Group's workforce, as appropriate, regarding changes in the Informatica Group's policies and procedures, or in Applicable Law and best practices, as they relate to data protection.

B. Complaint Handling

The Informatica Group has established a procedure for the receipt and processing of complaints regarding its processing of Employee Data and Business Contact Data. The Informatica Group's Employee Data Complaint Handling Standard is provided in Appendix B. The Informatica Group's Business Contact Data Complaint Handling Standard is provided in Appendix C.

C. Auditing Compliance

The Informatica Group implements a regular auditing program designed to ensure compliance with these BCR. This program sets the global minimum standard for conducting such audits. All employees involved in conducting such audits must comply with this standard. The Informatica Group's data protection council, being a sub-committee of the corporate compliance committee (which is a senior executive committee), will be responsible for implementing this auditing program. An audit shall be conducted no less than once every two years which will assess compliance with these BCR. Each individual audit may not cover all aspects of these BCR but the Informatica Group shall ensure that all aspects are monitored at appropriate regular intervals in the audit cycle.

The Informatica Group's Common Standard for Data Protection Audits is provided in Appendix D.

D. Data Protection Representatives

The Informatica Group has identified the Global Head of Privacy to act as a liaison between the highest level of management and processing personnel in each member of the Informatica Group and to assist in monitoring compliance with these BCR by that member. The Informatica Group's general counsel and/or Global Head of Privacy act as a resource and point of contact for, and communicate regularly with, the data protection representatives, who report into them.

The Global Head of Privacy shall inform and advise the highest level of management of and deal with supervisory authorities' investigations, and shall also monitor and report annually on compliance at a global level. Designated data protection representatives for each member of the Informatica Group shall deal with local complaints from data subjects, report major privacy issues to the Global Head of Privacy, and monitor compliance at a local level.

As part of this role, a designated data protection representative for a member of the Informatica Group will:

- To the extent supplementary measures or safeguards in addition to those envisaged under the BCR must be effected, propose supplementary measures or safeguards to the Global Head of Privacy;

- Promptly liaise with Informatica Group's general counsel and/or Global Head of Privacy in relation to identifying appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Informatica Group to enable them to fulfil their obligations under the BCR, where required.

- Notify the Global Head of Privacy, if an Informatica Group member has reason to believe that an Informatica Group member cannot fulfil its obligations under this BCR.

- Assess safeguards for the transfer of data and if required suspend the transfer or set of transfers impacted by the assessment.

- Liaise with the Informatica Group's general counsel and/or Global Head of Privacy, to inform all other Informatica Group members of assessments undertaken and supplementary measures adopted or, suspension of transfers.

Data protection representatives may be contacted directly by data subjects using the centralised email address (privacy@informatica.com) – and the relevant representative will handle any such communications as appropriate. Informatica Group will ensure that these contact details remain published on its website.

VIII. THE DUTY TO COOPERATE WITH DATA PROTECTION AUTHORITIES

The Informatica Group cooperates upon request with competent data protection authorities, including by submitting relevant data processing facilities and activities for audit by a competent Data Protection Authority ("**DPA**") and implementing the advice of a competent DPA regarding the requirements of these BCR and Applicable Law and abiding by the decisions of a competent DPA on any issue related to these BCR. Any dispute related to the DPA's exercise of supervision of compliance with the BCR will be resolved by the courts of the Member State of that DPA in accordance with that Member State's procedural law. The Informatica Group agrees to submit themselves to the jurisdiction of these courts.

The Informatica Group has established an internal privacy officers network (the "**PON**"). The local member of the PON will liaise with the relevant DPA, with input and support as necessary from the designated officer with primary responsibility for data protection for the Group and the Group data protection sub-committee (the "**DPS**"). For cross-border processing issues, the designated officer with primary responsibility for data protection will liaise with the lead DPA, with support from the relevant local members of the PON and the DPS.

IX. PROCEDURES FOR CHANGING THE BCR

The Informatica Group may, from time to time, need or want to update these BCR to reflect, *inter alia*, changes in the regulatory environment, the company structure, or the types of services and features offered. When the Informatica Group makes such a change or update, it will follow the procedures for recording and reporting such updates set forth in Appendix E.

X. ONGOING OBLIGATIONS

In the event that a non- EU member of the Informatica Group ceases to be part of the Informatica Group or to be bound by these BCR, that non- EU member of the Informatica Group will continue to apply the requirements of these BCR to the processing of any personal data transferred to it by means of these BCR unless, at the time of leaving the Informatica Group or ceasing to be bound by these BCR, that non- EU member of the Informatica Group has deleted or returned all such personal data to a member of the Informatica Group which remains bound by these BCR.

XI. CONTACT DETAILS

Informatica Ireland EMEA UC (registration number 566503) is the EU headquarters of the Informatica Group and the designated EU entity with delegated responsibilities for the BCR. Its principal office is located at:

Informatica Ireland EMEA UC,
Fifth Floor, 1 Windmill Lane,
SOBO District,
Dublin 2,
Ireland

Informatica Ireland EMEA UC can be contacted by emailing privacy@informatica.com. Details of other members of the Informatica Group may be found at Appendix A.

Appendix A

List of Entities in the Informatica Group

INFA entities that will be bound by BCR and jurisdiction in which established:	Company Address and Number	Functions
• Informatica Inc.	2100 Seaport Boulevard Redwood City CA 94063 United States TAX ID FEIN: 47-4330154	Parent entity listed on the New York Stock Exchange
○ **Informatica LLC** (US)	2100 Seaport Boulevard Redwood City CA 94063 United States FEIN: 77-0333710	✓ Research and Development ✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Product Management ✓ Sales
▪ I.D.I. Informatica Integration Ltd. (Israel)	121 Dvora Haneviah Street Kiryat Atidim, Building #8, 29th Floor Tel Aviv 6158101 Israel Company no: 512905936	✓ Research and Development ✓ Customer Services, Finance and Operations ✓ Product Management, ✓ Sales
▪ Informatica Development Ltd (UK)	Highlands House Basingstoke Road Spencers Wood, Reading, Berkshire England RG7 1NT United Kingdom Company no: 0569560	✓ Customer Services ✓ Finance and Operations ✓ Sales
▪ Informatica Software Ltd. (UK)	Highlands House Basingstoke Road Spencers Wood, Reading, Berkshire England RG7 1NT United Kingdom Company no: 03352679	✓ Research and Development ✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales
○ **Informatica Ireland EMEA UC** (Ireland)	1 Windmill Lane, Sobo District Dublin 2 Ireland Company no: 566503	✓ Research and Development ✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Product Management ✓ Sales
▪ Informatica Japan KK (Japan)	Level 26 Atago Green Hills MORI Tower 2-5-1 Atago, Minato-Ku Toyko 105-6226	✓ Research and Development, ✓ Finance and Operations, ✓ Marketing, ✓ Sales

INFA entities that will be bound by BCR and jurisdiction in which established:	Company Address and Number	Functions
	Japan Company no: 2011101046292	
▪ Informatica Business Solutions Private Ltd. (India)	No. 66/1, Bagmane Commerz 02 Bagmane Tech Park, C V Raman Nagar Bangalore 560 093 India Company no: U72200KA2003PTC031642	✓ Research and Development ✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Product ✓ Management Sales
▪ Informatica Software Ltd. (Canada)	1741 Lower Water Street, Suite 600 Halifax NS B3J 0J2 Canada Company no: 3012256	✓ Research and Development ✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales
▪ IS Informatica Software LTDA (Brazil)	Av. Das Nações Unidas, 12901 Torre Norte, terceiro andar (N-302) São Paulo 04578-000 Brazil Company no: 04.869.651/0001-73	✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales
▪ Informatica Software de Mexico S. A. de C.V. (Mexico)	c/o G.A. Asesores en Administracion, S.C. (Accountants) Boulevard Del Centro, No. 26 -14 Col. Boulevares, C.P. 53140 Naucalpan, Edo. De Mexico C.P. 53140 Mexico Company no: ISM071012-3Q0	✓ Sales
▪ Informatica Australia PTY Ltd (Australia, with a branch office in New Zealand)	Level 5 255 George Street Sydney NSW 2000 Australia ACN Company no: 114300686	✓ Research and Development ✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales
▪ Informatica S.E.A. Pte. Ltd (Singapore)	2 Shenton Way #18-01 SGX Centre I 068804 Singapore Company no: 200607626M	✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales
▪ Informatica Software Ltd. (Hong Kong)	Units 1106-1107, 11/F Berkshire House, 25 Westlands Road Quarry Bay Hong Kong Company no: 913204	✓ Research and Development ✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales
▪ Informatica Taiwan Co. Ltd. (Taiwan)	11F, No. 1 Song Zhi Road Xinyi District Taipei 11047 Taiwan Company no: 27993679	✓ Sales

INFA entities that will be bound by BCR and jurisdiction in which established:	Company Address and Number	Functions
▪ Informatica Data Integration Iberica S.L. (Spain)	C/ Jose Echegaray 8 Edificio 3 Bajo 3 Rozas de Madrid Spain Company no: ESB62198247	✓ Finance and Operations ✓ Marketing ✓ Sales
▪ Informatica France S.A.S. (France)	Tour CB 21 16 Place de l'Iris 92400 Courbevoie France Company no: FR48421340076	✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales
▪ Informatica GmbH (Germany)	Ingersheimer Str. 10 D-70499 Stuttgart Germany Company no: 99107/04411	✓ Research and Development ✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales
▪ Informatica Polska Sp.z.o.o.	ul. Kamienna 21 31-403 Kraków Poland Company no: 0000256448	✓ Research and Development ✓ Finance and Operations
▪ Informatica Software DMCC (Dubai)	Reef Tower Jumeirah Lake Towers PO Box 115 738 Dubai United Arab Emirates Company no: JLT1898	✓ Customer Services ✓ Marketing ✓ Sales
▪ Informatica Nederland B.V. (Netherlands)	Oval Tower, De Entrée 99-197 (9th floor) 1101 HE AMSTERDAM Netherlands Company no: 30148155	✓ Research and Development ✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales
▪ Informatica Software (Schweiz) GmbH (Switzerland)	City Center Stockerhof Dreikönigstrasse 31A CH-8002 Zürich Switzerland Company no: CHE-108.542.239	✓ Customer Services ✓ Sales
▪ Informatica Software Italia S.R.L.(Italy)	Piazza della Repubblica 14/16 20124 Milano Italy Company no: 05804300969	✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales
▪ Informatica Software Nederland B.V. (Netherlands)	Oval Tower, De Entrée 99-197 (9th floor) 1101 HE Amsterdam Netherlands Company no: 30148155	✓ Research and Development ✓ Customer Services ✓ Finance and Operations ✓ Marketing ✓ Sales

INFA entities that will be bound by BCR and jurisdiction in which established:	Company Address and Number	Functions
▪ Informatica Software Pty Ltd (South Africa)	9 Kinross Street Germiston South Gauteng 1401South Africa Company no: 2011/128121/07	✓ Sales
▪ Informatica Sweden AB (Sweden)	Grev Turegatan 30, 11438 Stockholm Sweden Company no: 556793-1091	✓ Customer Services ✓ Marketing ✓ Sales
▪ Info Corp. Portugal Unipessoal Lda. (Portugal)	Building Amoreiras Square Rua Carlos Alberto da Mota Pinto n° 17 3rd Floor A, Amoreira 1070-313Lisboa Portugal Company no: PT507752422	✓ Customer Services
▪ Informatica Belgie BVBA (Belgium)	Brusselstraat 51 2018 Antwerpen Belgium Company number no: 0472.109.292	✓ Customer Services ✓ Research and Development ✓ Sales
▪ INFA Denmark ApS	Lyskær 3C, 2. 2730 Herlev Denmark Company no: 43280910	✓ Sales
▪ Informatica Software Services de México, S. A. de C.V.. (Mexico)	c/o G.A. Asesores en Administracion, S.C. (Accountants) Boulevard Del Centro, No. 26 -14 Col. Boulevares, C.P. 53140 Naucalpan, Edo. De Mexico C.P. 53140 Mexico Company no: ISS071012-NE6	✓ Sales
▪ Privitar Limited (UK with France branch office)	Salisbury House Station Road Cambridge CB1 2LA Company no: 09305666	✓ Research and Development ✓ Sales
▪ Privitar, Inc. (US)	200 Portland Street Boston, MA 02114 FEIN: 37-1881002	✓ Research and Development ✓ Sales
▪ Privitar Polska sp. z.o.o. (Poland)	ul. TOWAROWA, nr 28, lok. kod 00-839, poczta WARSZAWA, kraj POLSKA	✓ Research and Development ✓ Sales

Appendix B

Employee Data Complaint Handling Standard

Employee Data Complaint Handling Standard

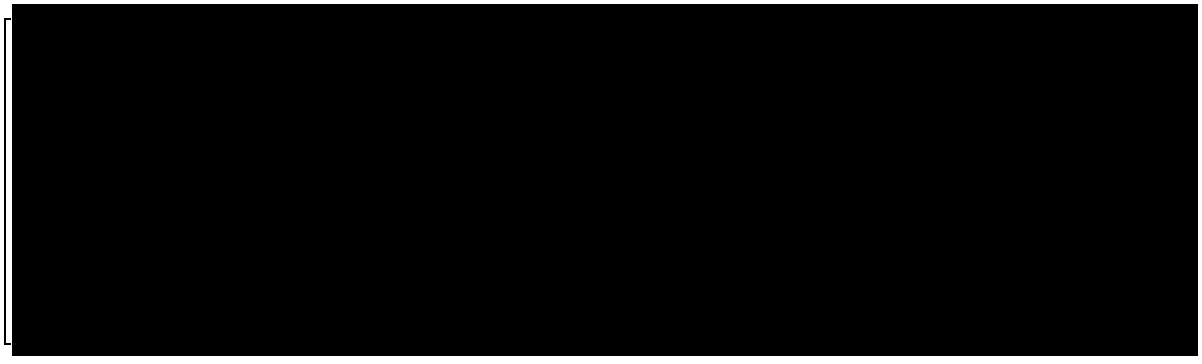

Table of Contents

TABLE OF CONTENTS 2
PURPOSE 1
SCOPE 1
STANDARD 1
STANDARD DETAILS 1
1 Escalation Process 1
2 External Escalation 2
3 Recording Complaints 3
COMPLIANCE 3
1 Enforcement 3
2 Training 3
3 Record-Keeping 3
4 Audits 3
MODIFICATIONS TO THE STANDARD 3
RELATED POLICIES, STANDARDS AND PROCEDURES 4
DOCUMENT CONTROL AND REVISION HISTORY 4

Purpose

Informatica is committed to protecting the privacy of its employees in accordance with applicable law (including without limitation, those of the EU and EU member states and the Informatica Group Controller Binding Corporate Rules (where applicable)). This standard sets the global minimum standard for handling complaints from employees about the processing of Employee Data and provides guidance to employees about how they can ask a question, raise a concern, or submit a complaint regarding Informatica's processing of their own Employee Data.

Scope

This standard applies to all Informatica employees and should be read in conjunction with Informatica's Employee Data Privacy Policy and associated standards. Please refer to the Employee Data Privacy Policy for definitions of any capitalized terms used in this standard.

Standard

Informatica has established an internal escalation process designed to ensure that employees have an effective and comfortable means of raising, and receiving a prompt reply to, their questions, concerns or complaints about the processing of Employee Data. Employees may also have the right to lodge complaints with a supervisory authority or through the courts.

Standard Details

1 Escalation Process

1.1 Human Resources

Employees should raise questions, concerns, or complaints regarding how Informatica processes their Employee Data by email to the HR department or through the Informatica Hotline http://informatica.ethicspoint.com. Contact information varies depending on the employee's country. The employee will find suitable contact information and options on how to report online or by phone on the Informatica Hotline website. The HR department will respond to inquiries, address concerns, and resolve complaints consistent with its data protection policies, standards, and procedures.

The HR department will endeavor to respond to a complaint within one month of the date the complaint is received. Where the HR department does not respond to the complaint within this timeframe, employees may contact Informatica's legal department directly (see Legal Department Review below) and also has the right to lodge a complaint to the competent supervisory authority, a court of competent jurisdiction, or both (see External Escalation below). If the complaint is too complex to allow a response within one month, that period may be extended by two additional months where necessary. The HR department will inform the employee concerned of any such

extension within one month of receipt of the request, together with the reasons for the delay. If the complaint is rejected, the HR department will inform the employee within one month of receipt of the complaint of its reasons for not taking action and the possibility available to the employee of lodging a complaint to the competent supervisory authority, a court of competent jurisdiction, or both (see External Escalation below). The complaint is deemed to be closed on the date Informatica issues its final response to the employee concerned.

Where a complaint is considered as justified: Informatica will (i) take necessary action to correct or remedy the issue; and (ii) be liable for any appropriate sanction and material or non-material damage suffered by the employee as a result in accordance with the Informatica Group Controller Binding Corporate Rules.

1.2 Legal Department Review

If a complaint is rejected or an employee is otherwise not satisfied with the manner in which Informatica addresses the issue, the employee may raise it directly with Informatica's legal department by emailing: privacy@informatica.com. Informatica's legal department will endeavor to respond to a complaint within one month of the date the complaint is received. If the complaint is too complex to allow a response within one month, that period may be extended by two additional months where necessary. Informatica's legal department will inform the employee concerned of any such extension within one month of receipt of the request, together with the reasons for the delay. The complaint is deemed to be closed on the date Informatica's legal department issues its final response to the employee concerned. The relevant employee nonetheless has a right to lodge a complaint to the competent supervisory authority, a court of competent jurisdiction, or both (see External Escalation below).

2 External Escalation

Every employee in an EU Member State has the right to lodge a complaint with an appropriate supervisory authority (being the supervisory authority of the EU member state of (i) the employee's habitual residence, (ii) the employee's place of work, or (iii) the place of alleged infringement, at the employee's option, regarding Informatica's processing of Employee Data if the employee believes that the processing of Employee Data relating to him or her infringes applicable EU or EU member state data protection law. Employees may also lodge a claim with a court of competent jurisdiction (being the courts (i) where the EU member of the Informatica Group responsible for the violation has an establishment, or (ii) where the employee has his / her habitual residence, at the employee's option).

It is at the option of the employee whether to raise a complaint with either a supervisory authority, a court of competent jurisdiction, or both.

3 Recording Complaints

Informatica will document formal employee concerns or complaints regarding the processing of Employee Data, including the substance of the concern or complaint, the steps taken to respond to it, and the resolution of the concern or complaint.

Compliance

1 Enforcement

All employees must comply with this standard. In particular, human resources and the legal department must receive, and process inquiries, concerns, and complaints as described herein and seek to resolve them consistent with Informatica's data protection policies, standards, and procedures. Questions regarding how this standard applies, or what it requires in a specific context, should be directed to Informatica's legal department. Failure to comply with this standard may result in disciplinary action, up to and including termination of employment.

Compliance with this standard does not impact on an employee's right to lodge complaints with a supervisory authority or through the courts.

2 Training

Informatica will develop and provide to pertinent employees training regarding this standard.

3 Record-Keeping

Informatica will maintain adequate and where necessary, up to date records to demonstrate compliance with this standard.

4 Audits

To help ensure compliance with this standard, Informatica, in accordance with its audit program, will review Employee Data processing activities and practices on a regular basis. Informatica will, where necessary, establish and implement a corrective action plan designed to help ensure and improve compliance with this standard.

Modifications to the Standard

Informatica reserves the right to modify this standard, for example, to comply with changes in laws, regulations, Informatica's practices, procedures and organizational structure or requirements imposed by data protection authorities. Changes to the standard shall be applicable on the effective date of implementation. Informatica will provide notice of material changes in accordance with its internal notice procedures.

Related Policies, Standards and Procedures

- Employee Data Privacy Policy

Document Control and Revision History

Date	Participants	Scope
[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
4/30/2023	Joe Bracken	V1.4 – annual review.

Appendix C

Business Contact Data Complaint Handling Standard

Business Contact Data Complaint Handling Standard

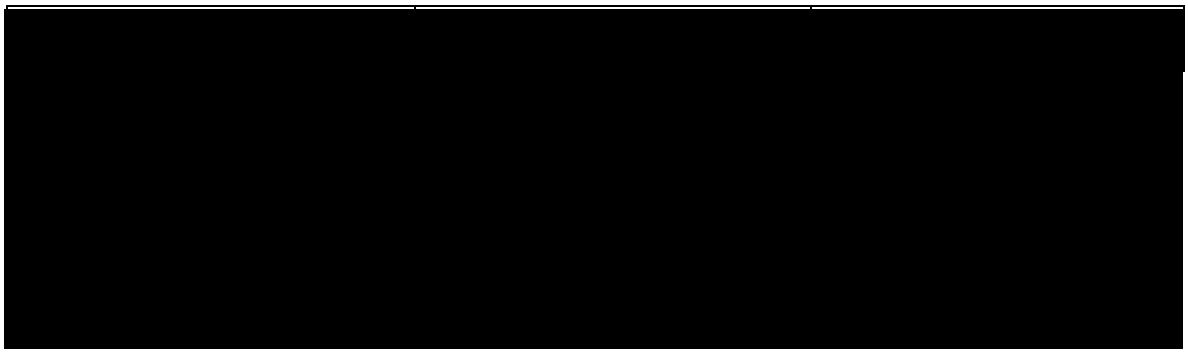

Table of Contents

TABLE OF CONTENTS 1
PURPOSE 2
SCOPE 2
STANDARD 2
STANDARD DETAILS 2
1 Process 2
2 External Escalation 3
3 Recording Complaints 4
COMPLIANCE 4
MODIFICATIONS TO THE STANDARD 4
RELATED POLICIES, STANDARDS AND PROCEDURES 5
DOCUMENT CONTROL AND REVISION HISTORY 5

Purpose

Informatica is committed to protecting the privacy of its Business Contacts in accordance with applicable law (including without limitation, those of the EU and EU member states and the Informatica Group Controller Binding Corporate Rules (where applicable)). This standard sets the global minimum standard for handling complaints from Business Contacts about the processing of Business Contact Data.

Scope

This standard applies to all Informatica employees and should be read in conjunction with Informatica's Business Contact Data Internal Privacy Policy and associated standards. Please refer to the Business Contact Data Internal Privacy Policy for definitions of any capitalized terms used in this standard.

Standard

Informatica has established an escalation process designed to ensure that Business Contacts have an effective, readily-available means of raising, and receiving a prompt reply to, their questions, concerns or complaints about the processing of Business Contact Data. Business Contacts may also lodge complaints with a supervisory authority or through the courts.

Standard Details

1 Process

1.1 Making a Complaint

Business Contacts can raise questions or concerns or lodge complaints regarding Informatica's processing of Business Contact Data by emailing privacy@informatica.com or by writing to Informatica at Informatica EMEA Headquarters, Informatica Ireland EMEA UC, (Fifth Floor), 1 Windmill Lane, SOBO District, Dublin 2, Ireland. Business Contacts can also raise a concern directly with their primary business contact at Informatica, who will initiate a formal review process by referring the concern to privacy@informatica.com. Nothing in this standard impacts on a Business Contact's right to lodge a complaint with a supervisory authority or through the courts.

1.2 Legal Department Review

Informatica's legal department will review Business Contacts' complaints regarding Informatica's use, collection, and/or retention of Business Contact Data to ensure that the processing of

Business Contact Data is consistent with Informatica's data protection policies, standards, and procedures. In particular, the legal department will confirm that the Business Contact Data collected is limited to the degree practicable to accomplish the legitimate purpose(s) for which the data is processed.

Informatica's legal department will endeavor to respond to a complaint within one month of the date the complaint is received. Where Informatica's legal department does not respond to the complaint within this timeframe, the Business Contact has the right to lodge a complaint to the competent supervisory authority, a court of competent jurisdiction, or both (see External Escalation below). If the complaint is too complex to allow a response within one month, that period may be extended by two additional months where necessary. Informatica's legal department will inform the Business Contact concerned of any such extension within one month of receipt of the request, together with the reasons for the delay. If the complaint is rejected, Informatica's legal department will inform the Business Contact within one month of receipt of the complaint of its reasons for not taking action and the possibility available to the Business Contact of lodging a complaint to the competent supervisory authority, a court of competent jurisdiction, or both (see External Escalation below). The complaint is deemed to be closed on the date Informatica issues its final response to the Business Contact concerned.

Where a complaint is considered as justified: Informatica will (i) take necessary action to correct or remedy the issue; and (ii) be liable for any appropriate sanction and material or non-material damage suffered by the Business Contact as a result in accordance with the Informatica Group Controller Binding Corporate Rules.

2 External Escalation

If a Business Contact's complaint regarding Informatica's processing of Business Contact Data is not resolved, the Business Contact may register the complaint with a competent supervisory authority (being the supervisory authority of the EU member state of (i) the Business Contact's habitual residence, (ii) the Business Contact's place of work, or (iii) the place of alleged infringement, at the Business Contact's option). The legal department will notify the Business Contact of this right to register a complaint. The Business Contact may also lodge a claim with a court of competent jurisdiction (being the courts (i) where the EU member of the Informatica Group responsible for the violation has an establishment, or (ii) where the Business Contact has his / her habitual residence, at the Business Contact's option).

It is at the option of the Business Contact whether to raise a complaint with either a supervisory authority, a court of competent jurisdiction, or both.

3 Recording Complaints

Informatica will document formal customer concerns or complaints regarding the processing of Business Contact Data, including the substance of the concern or complaint, the steps taken to respond to it, and the response to the request.

Compliance

Enforcement

All employees must comply with this standard. In particular, the legal department must receive and process inquiries, concerns, and complaints as described herein and seek to resolve them consistent with Informatica's data protection policies, standards, and procedures. Questions regarding how this standard applies, or what it requires in a specific context, should be directed to Informatica's legal department. Failure to comply with this standard may result in disciplinary action, up to and including termination of employment.

Training

Informatica will develop and provide to pertinent employees training regarding this standard.

Record-Keeping

Informatica will maintain adequate and where necessary, up to date records to demonstrate compliance with this standard.

Audits

To help ensure compliance with this standard, Informatica, in accordance with its audit program, will review Business Contact Data processing activities and practices on a regular basis. Informatica will, where necessary, establish and implement a corrective action plan designed to help ensure and improve compliance with this standard.

Modifications to the Standard

Informatica reserves the right to modify this standard, for example, to comply with changes in laws, regulations, Informatica's practices, procedures and organizational structure or requirements imposed by data protection authorities. Changes to the standard shall be applicable on the effective date of implementation. Informatica will provide notice of material changes in accordance with its internal notice procedures.

Related Policies, Standards and Procedures

- Business Contact Data Internal Privacy Policy

Document Control and Revision History

Date	Participants	Scope
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
4/30/2023	Joe Bracken	V16 – annual review.

Appendix D

Common Standard: Data Protection Audits

Common Standard: Data Protection Audits

Table of Contents

TABLE OF CONTENTS 1
PURPOSE 2
SCOPE 2
STANDARD DETAILS 2
1 Data Protection Council Oversight 2
2 Audit Parameters 3
3 Audit Objectives 3
4 Audit Methodology 4
5 Audit Reports 4
6 Investigative Audits 4
COMPLIANCE 5
MODIFICATIONS TO THE STANDARD 5
DOCUMENT CONTROL AND REVISION HISTORY 6

Purpose

Informatica recognizes and respects the data protection and privacy rights of its employees and all parties with which it does business. Informatica conducts regular audits to raise awareness regarding its privacy and data protection practices and examine its policies, procedures, systems, and records in order to assess its compliance with applicable privacy and data protection laws (including without limitation, those of the EU and EU member states and the Informatica processor and controller binding corporate rules (where applicable)) and other aspects of Informatica's policies, standards and procedures. This procedure sets the global minimum standard for conducting such data protection audits.

Scope

This procedure applies to all Informatica employees.

Standard Details

1 Data Protection Council Oversight

The data protection council, being a sub-committee of the corporate compliance committee (which is a senior executive committee), ("**Council**") will meet regularly or on specific request from the Global Head of Privacy to establish an audit plan and schedule designed to result in a regular, no less than once every two years, thorough examination of Informatica's data protection policies, procedures, systems, and records, Informatica's Binding Corporate Rules (including methods of ensuring that corrective actions will take place), and Informatica personnel's general awareness regarding its data protection obligations. Audits will focus on the processing and flow of personal data into, within, and out of Informatica and may be structured around one or more particular data processing principles (e.g., purpose limitation or data minimization) relating to the processing of personal data. In determining the scope and subject matter of the audit, the Council will take into account, among other factors, areas that involve high risk processing or special categories of personal data, areas with respect to which remedial or corrective action has recently been undertaken, areas that have been the subject of data subject complaints or concerns, areas in which guidance or additional best practices have recently become available, and prior audits conducted with the objectives of regularity and thoroughness in mind. Informatica's Processor and Controller Binding Corporate Rules will be audited on a regular basis and no less than once every two years. Each individual audit may not cover all aspects of the BCRs but the Council shall ensure that all aspects are monitored at appropriate regular intervals in the audit cycle.

For each audit, the Council will determine the scope of the audit, identify the controls and standards against which to audit and delegate responsibility for conducting the audit. The Council and the Global Head of Privacy will receive a final report of each audit. The Council will be responsible for considering the implementation of appropriate improvements and remedial actions. Such improvements and remedial action identified as a result of each audit will, as appropriate, be shared with the board of the relevant Informatica group member and disseminated through the Informatica group including (where relevant) by way of employee training and through Informatica's internal privacy officers network. Where appropriate, the results of an audit may be communicated to the boards of Informatica US and Informatica Ireland, which are the parent entities of all Group subsidiaries.

2 Audit Parameters

For the purposes of this standard, an audit is a systematic and independent inspection and examination to determine whether activities within the defined scope of the audit involving the processing of personal data are carried out in accordance with Informatica's policies and meet the requirements of applicable laws (including without limitation, applicable EU or EU member state laws).

3 Audit Objectives

In addition to ordinary audit objectives, data protection audits will have the following objectives:

- Raise awareness and increase understanding among Informatica personnel regarding Informatica's data protection obligations and practices;
- Determine how Informatica's resources and assets are managed to meet data protection standards and achieve implementation of the data protection principles;
- Verify that there is a formal, documented, up-to-date data protection system (i.e., policies, procedures, practices, and personnel) in place;
- Detect irregularities, system weaknesses, or inadequate practices regarding Informatica's handling and processing of personal data;
- Identify risks of possible non-compliance with or contravention of applicable laws; and,
- Recommend changes, enhancements, remedial actions, and best practices to improve Informatica's compliance with the policies and applicable laws.

4 Audit Methodology

The Council will ensure that all audits are independent and follow effective audit methodologies that it has previously found effective and may consider the use of a combination of questionnaires, document reviews, process and procedure inspections, technical tests, interviews, and site visits.

5 Audit Reports

5.1 Draft Reports

The Council will, when appropriate, delegate responsibility for producing a draft audit report that contains requests for further clarification or confirmation of facts or practices. The Council will provide the audited office, business unit, or other entity with the draft report and request that it provide clarification and confirmation as necessary and give it an opportunity to submit its own views of the areas and practices assessed in the audit.

5.2 Final Reports

The Council will delegate responsibility for generating a final report as the official record of the audit. Each final report shall contain a description of the scope of the audit, the methodology or methodologies employed, an overall conclusion, findings, and recommendations. At the Council's request, a meeting may be called at which the personnel responsible for conducting the audit may provide a briefing on the audit. Where, and to the extent, appropriate, Informatica will also make available to relevant Customers an abridged version of the final report, or an appropriate summary or portion of a final report that relates to Informatica's processing of personal data as a data processor on behalf of its Customers, subject to appropriate confidentiality obligations being agreed by the relevant Customer. Informatica will also make appropriate final reports available to competent data protection authorities upon request.

6 Investigative Audits

In addition to the planned audits described above, the Council or Informatica's legal department may, as appropriate, request additional investigative audits in response to particular complaints, reports, or incidents suggesting an area of high risk or potential non-compliance. Such audits will employ the methodologies and seek to achieve the objectives described above on an expedited basis.

Upon request, Informatica may also provide the competent data protection authorities with copies of the final reports of such audits. In the event that the competent data protection

authorities carry out their own data protection audits, all concerned affiliates and Informatica personnel will support and cooperate with the competent authorities in their conduct of such audits. Informatica will abide by and seek to implement faithfully the advice and recommendations of the competent data protection authorities regarding issues presented by such audits.

7 External Audits

Informatica will allow relevant data processing activities to be audited upon the request of a Customer on a schedule mutually agreed upon by Informatica and the Customer. Informatica will also allow relevant data processing activities to be audited by a competent supervisory authority upon the request of such authority.

Compliance

Enforcement

All employees must comply with this standard. Questions regarding how the standard applies, or what it requires in a specific context, should be directed to Informatica's legal department. Violation of this standard may result in disciplinary action, up to and including termination of employment.

Training

Informatica will develop and provide to pertinent employees training regarding this standard.

Record-Keeping

Informatica will maintain adequate and where necessary, up to date records to demonstrate compliance with this standard.

Modifications to the Standard

Informatica reserves the right to modify this standard, for example, to comply with changes in laws, regulations, Informatica's practices, procedures and organizational structure or requirements imposed by data protection authorities. Changes to the standard shall be applicable on the effective date of implementation. Informatica will provide notice of material changes in accordance with its internal notice procedures.

Document Control and Revision History

Date	Participants	Scope
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
4/30/2023	Joe Bracken	V1.4 Annual review. Minor changes.

Appendix E

Procedures for Recording and Reporting Updates to these BCR

A. Authorizing a Change

Any change or update to these BCR must be authorized by the general counsel, in consultation with the designated officer with primary responsibility for data protection.

B. Recording Changes, Maintaining Records

The Informatica Group's designated officer with primary responsibility for data protection will keep track of and record any updates to the BCR. Such officer will maintain all past and current versions of the BCR, together with records reflecting the date each change was made. Such versions and records will be made accessible to employees, business contacts, and competent DPAs.

C. Reporting Changes

The Informatica Group reports as set forth in this section changes to the BCR to all group members and to competent DPAs. The Informatica Group reports changes to group members without undue delay by communication to the designated data protection representative for each Informatica Group member. The Informatica Group will report (i) any changes to the BCR which would affect the level of protection afforded under the BCR or significantly affect the BCR, promptly via the competent DPAs and (ii) any other changes to the BCR or to the list of Informatica Group members via the competent DPAs on an annual basis, inclusive of an explanation for the updates.

E. Maintaining Compliance

The Informatica Group will not transfer Employee Data or Business Contact Data to a new member of the Informatica Group under these BCR until the new member is effectively bound by the BCR and is compliant with their terms.

Appendix F

Business Contact Data and Employee Data*

Processing Activity	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
Operations, Marketing, Partner / Vendor Relationship	Customer and prospect leads management and communication; direct marketing campaigns and sales; processing of payment services; entering into and maintaining business relationships with vendors, advisors and business partners	1. Identifiers such as name.	Informatica Group's vendors, business partners, advisors, customers, prospects **(Business Contact Data)**
		2. Contact information such as postal address, telephone number, online identifier, and email address.	
		3. Identifying metadata such as Internet Protocol address.	
		4. Gender.	
		5. Commercial information such as records of products or services purchased or considered.	
		6. Internet or other electronic network activity information, such as search history and interaction with our websites, cloud services and other applications, or advertisements.	
		7. Geolocation data, such as the physical location of a person or device.	
		8. Electronic, visual, or other similar information, such as photos, videos, or webcasts from events.	

Processing Activity	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		9. Professional or employment related information, such as current or past employment status and job role.	
		10. Inferences drawn from the personal information above reflecting your preferences, characteristics, and behaviour.	
		11. Marketing preferences.	
		12. Communication preferences, such as the content of communication with an Informatica staff member.	
HR processing activities	Recruitment management; employee records management; payroll management; referral programs; training management; employee career management; background checks; immigration checks; employee absence and working time management; performance and evaluation; travel and expenses management; employee management.	1. Identifiers such as name.	Informatica Group employees (and their declared relatives); candidates; agents; operators. **(Employee Data)**
		2. Contact information such as postal address, telephone number, and email address.	
		3. Identifying metadata such as IP Address.	
		4. Directly collected recruitment information, such as resume (including education, employment, and military history), cover letter, references,	

Processing Activity	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		employment application and notes regarding whether a candidate is appropriate for the work.	
		5. Government or national identification information, such as your national insurance or social security number, and visas and work authorization.	
		6. Payroll information, such as banking and direct deposit forms, salary, tax forms, expense reimbursement records, and vacation and PTO balances.	
		7. Performance information, such as performance reviews and disciplinary reports.	
		8. Benefits information, such as benefits elections, beneficiaries, spousal or partner information, dependent information, disability status, and trade union membership where required.	
		9. Workforce identification information, such as photograph.	
		10. Where required by local law or to support our diverse workplace initiatives, demographic information such as gender and data revealing racial or ethnic origin.	
		11. Information about use of company technology and resources, including	

Processing Activity	Purpose of Processing	Categories of Personal Data	Categories of Data Subjects
		our intranet, our talent acquisition and recruiting websites, email, instant messaging, file share and employee collaboration platforms, IT help desk, and employee training tools.	
		12. Images or video footage capture by surveillance equipment such as cameras and CCTV we use to secure the entrances and exits of some Informatica offices, prevent theft of Informatica property, and protect the personnel and visitors at those offices.	
		13. Indirectly collected recruitment information, such as information from references, background checks, and recruiting platforms through which applicants have submitted their application.	
		14. Data relating to benefits from benefits providers and brokers as part of resolving eligibility for or questions concerning those benefits.	

* The BCR apply to all transfers among the members of the Informatica Group and within those EEA and non-EEA countries.

Appendix G

Supplementary Measures

Supplementary Measures – Transfers in Informatica Group

The Informatica Group, when transferring personal data internally to other Informatica entities, has put in place the following supplementary measures, where necessary to supplement the safeguards under the BCR:

Technical Measures

In accordance with Informatica Group's Global Security Office's 2021 Data Security & Protection Standards, all personal data are classified "Restricted" and require confidentiality terms before sharing, encryption at storage and at rest, and labelling. The said standards and the Informatica's Information Security Policy outline details including data handling requirements and controls, access controls, labeling, disclosure, shipping and handling, destruction and disposal, physical security, and cryptography.

Contractual Measures

Informatica Group's Interaffiliate Data Processing and Transfer Agreement (which is to incorporate Informatica's Intra-Group Agreement) requires each data importer to make all commitments required under the standard contractual clauses approved by the European Commission, including for clarity the obligation to be liable for damages it causes, submitting itself to jurisdiction of the competent supervisory authority, a warranty that the laws and practices in the destination do not prevent it from fulfilling its obligations, and an obligation to review and notify the data exporter of legally binding requests for personal data transferred.

In accordance with Informatica Group's Interaffiliate Data Processing and Transfer Agreement, any Informatica Group member acting as data importer agrees:

i. No transfer is made to a Informatica Group member unless the Informatica Group member is effectively bound by the BCR and can deliver compliance.

ii. The data importer is to promptly inform the data exporter if it is unable to comply with the BCR, for whatever reason.

iii. Where the data importer is in breach of the BCR or unable to comply with them, the data exporter will suspend the transfer.

iv. The data importer shall, at the choice of the data exporter, immediately return or delete the personal data that has been transferred under the Interaffiliate Data Processing and Transfer Agreement in its entirety (including any copies of the personal data), where:

- the data exporter has suspended the transfer, and compliance with the BCR 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; or

- the data importer fails to comply with a binding decision of a competent court or competent supervisory authority regarding its obligations under the BCR.

The data importer shall certify the deletion of the personal data to the data exporter upon request. Until the personal data is deleted or returned, the data importer shall continue to ensure compliance with the BCR. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with the BCR, and will only process the data to the extent and for as long as required under that local law.

Organizational Measures

In accordance with Informatica Group's Interaffiliate Data Processing and Transfer Agreement, the data importer commits to organizational measures to safeguard European personal data, including measures to prevent retrieval of personal data from disposed or reused media, proper management of personal data security incidents, least privilege access control for personal data, a security awareness and training program for all personnel, and a business continuity and disaster recovery program. Any Informatica Group member acting as data importer is required to promptly notify the data exporter if, when using the Interaffiliate Data Processing and Transfer Agreement as a tool for transfers, and for the duration of the said agreement, 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 said agreement and / or the BCR, including following a change in the laws in the third country or a measure (such as a disclosure request). This information should also be provided to the Informatica Ireland. Upon verification of such notification, the Informatica Group member acting as data exporter, along with Informatica Ireland and the relevant PON function, will commit to promptly identify supplementary measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the Informatica Group member acting as data exporter and/or data importer, in order to enable them to fulfil their obligations under the BCR. The same applies if an Informatica Group member acting as data exporter has reasons to believe that an Informatica Group member acting as its data importer can no longer fulfil its obligations under this BCR.

Where the Informatica Group member acting as data exporter, along with Informatica Ireland and the relevant PON function, assesses that the BCR – 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, it 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 Informatica Group member acting as data exporter has to end the transfer or set of transfers if the BCR 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 Informatica Group member acting as data exporter, be returned to it or destroyed in their entirety. Informatica Ireland and the relevant PON function will inform all other Informatica Group member 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 Informatica Group member or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

Supplementary Measures – Transfers to Vendors

The Informatica Group, when transferring personal data to vendors, may require of vendors, as part of its vendor risk assessment or diligence program, the below standard minimum vendor security requirements, where necessary to supplement the safeguards under the BCR.

The following standard minimum vendor security requirements may vary in older agreements, negotiated agreements, or agreements based on the vendor's paper. The Informatica Group attempts to secure similar protections to the below in these other agreement types.

Technical Measures

The Informatica Group may require vendors to:

- Maintain and follow screening procedures and industry standard employment verification requirements for all new employees and contractors hired, including conducting background checks (including criminal background checks) to the extent permitted by local laws and proof of identity validation, and additional checks that the vendor deems necessary. The vendor will periodically validate these requirements and perform rechecks as it deems necessary. The vendor must ensure that vendor representatives authorized to process personal data have committed in writing to maintain the confidentiality of Informatica personal data or are under an appropriate statutory obligation of confidentiality.

- Continuously monitor for new risks to personal data, both internally and externally, including, without limitation, up-to-date controls to protect all vendor systems from malware, ransomware, and unauthorized software, including prompt implementation of all security patches when issued.

- Maintain a compliance program to conduct due diligence and monitor the security and processing activities of its subprocessors or subcontractors. The vendor must ensure that security and data privacy requirements are included in third party contracts and these commitments are reasonably monitored throughout the term of services provided.

- Maintain an awareness and training program for the vendor representatives who may have access to personal data, which includes compliance with Applicable Law and information security industry standards and best practices, including, but not limited to, phishing and social engineering, strong passwords, removable media, and emerging threats and trends, and which is provided to the vendor representatives upon hire and on an annual basis.

- Maintain an asset inventory that accurately reflects the vendor systems used to process personal data (including information systems, cloud services, and infrastructure where relevant), including when an asset is installed, removed, or updated.

- Ensure that a secure baseline configuration is established, maintained, and reviewed periodically for all vendor systems used to provide the products or services to Informatica.

- Not use mobile devices, tablets, personal laptops or other mobile computing devices ("Mobile Devices") to process personal data without Informatica's prior written consent. In the event Informatica provides consent, the vendor must ensure that, in addition to the safeguards directly above, all Mobile Devices utilize (i) whole-disk encryption using an industry standard method; (ii) automatic locking of the Mobile Device after periods of inactivity of five minutes or less; (iii) password login using at least a 6-digit numeric password; and (iv) remote-wipe capability in the event of a loss or theft of the Mobile Device.

- Encrypt personal data in transit and at rest using a generally recognized encryption standard, including encryption of all Mobile Devices (if applicable), removable media, backup copies and systems containing or processing personal data, with a minimum of 256 AES bit Encryption and TLS 1.2 or above.

- Maintain password management measures requiring at a minimum (i) reasonable password complexity and account lockouts after periods of inactivity and multiple unsuccessful attempts for all users; and (ii) all third party-supplied default passwords and other security parameters on any vendor systems or third-party software are replaced with a unique password prior to processing personal data.

- Maintain a documented access management process which differentiates between regular and privileged account management. Authentication to vendor systems will require unique passwords and role-based access control, and where available, single sign-on (SSO) and federated identity management (FIM). Multi-factor authentication will be used for (i) the vendor's privileged users, (ii) remote access to vendor systems, and (iii) access to personal data and confidential information. Access to and activity on vendor systems must be monitored appropriately, including maintaining audit trails for access and activity logs for a minimum of thirteen (13) months or other time period required by Applicable Law.

- Ensure that the vendor or its representatives have access controls which are designed to limit access to personal data to the vendor's representatives on a need-to-know basis and only as necessary for the performance of the services under the relevant agreement. Access must be removed or revoked within twenty-four (24) hours after the termination of employment, termination or expiration of services, or reassignment of duties. The vendor will perform quarterly access reviews for privileged and other accounts that have access to personal data and systems.

- Ensure all personal data is compartmentalized or otherwise logically distinct from, and in no way commingled with, other information of the vendor or its personnel, suppliers, customers or other third parties.

- Maintain necessary technical and organizational measures to prevent personal data from (a) being accidentally or illegally destroyed, lost or manipulated, (b) being shared with any

third parties, (c) being subject to unauthorized use or disclosure, or (d) being processed contrary to Applicable Law.

- Apply industry standard data sanitization practices (such as NIST 800-88 or an equivalent) to ensure the secure destruction of all personal data as soon as it is no longer required for a valid business purpose. This extends to all electronically stored information, paper assets, and other physical media, such as backup tapes or external drives.

- Maintain a documented change management process that ensures proposed changes to vendor systems, including any applications or software, are validated, authorized, tested in a non-production environment, and approved before deployment. The process should include handling emergency changes to vendor systems.

- Maintain vulnerability management procedures and tools which continuously monitor and remediate vendor systems for vulnerabilities including but not limited to, open ports, misconfigurations, insecure or missing authorization, insecure cryptography, cross-site scripting, code injections, and other vulnerabilities. The vendor must promptly notify Informatica of any known or suspected material vulnerabilities that it discovers affecting vendor systems or personal data.

- Follow industry standard secure software development practices (such as from Open Web Application Security Project "OWASP" or an equivalent) to develop software, services, or deliverables in a secure manner. The vendor will have controls in place to track and manage changes to software code and configurations. The vendor will maintain an inventory of any open-source code or third-party libraries (collectively, "TPLs") used in its products or services and have measures in place for security of the TPLs. Within thirty (30) days of Informatica's written request, the vendor will provide a summary of its software development practices to Informatica.

- Maintain policies and procedures for business continuity and disaster recovery that are documented, approved, and reviewed annually. The business continuity plan should ensure the availability and prompt restoration of personal data, including appropriate security measures for backups and networks. The vendor must test the business continuity plan at least on an annual basis. For any hosted services provided by the vendor, the specific recovery point objective ("RPO") should be a minimum of twenty-four (24) hours and the recovery time objective ("RTO") should be a minimum of eight (8) hours.

- Maintain a security incident response plan including mitigation, remediation, customer communication, and a post-incident review in the event of an actual or suspected security breach or other significant security incident.

- Maintain data loss prevention measures to prevent the unauthorized use, access, disclosure of or loss of personal data by email, portable storage devices (including portable hard drives, flash drives, and thumb drives), and other means.

- Maintain physical controls per industry standards designed to secure relevant facilities, infrastructure, data centres, hard copy files, servers, backup systems, and equipment used

to process personal data, including controls to prevent, detect, and respond to intrusions or other system failures.

Members of the Informatica Group may implement the following measures to protect data transferred to vendors:

- Informatica's information security team reviews the vendors' security protections prior to signing and may insist on improvements where appropriate as a condition of signing. In some cases, Informatica may choose not to use a vendor or to retain additional responsibility ourselves, such as pseudonymization prior to transmission, in order to minimize risk from vendors with potential gaps in their risk treatment measures.

- State-of-the-art encryption measures for data in transit to vendors, and verification of the identity of the vendor before transmission.

- Maintenance of logs reflecting access by vendors to Informatica's systems/data and permits access only on a need-to-know basis.

Contractual Measures

The Informatica Group may require of vendors:

- Contractual obligations reflecting any supplemental technical measures (described above), or organizational security measures (described below).

- Contractual representation that it has not received requests from public authorities that have undermined the vendor's ability to adequately protect personal data.

- Contractual obligation to process personal data solely for the purposes of performing the obligations and providing the services and/or deliverables to Informatica under the relevant agreement during the term of that agreement.

- Contractual obligation for the vendor to comply with any additional instructions related to the transferred data communicated by Informatica on behalf of a European customer/data subject.

- Contractual right of Informatica to conduct audits for compliance with supplemental measures.

- Contractual right of Informatica to immediately terminate the underlying contract or suspend data transfers if the vendor breaches its contractual obligations under the standard contractual clauses approved by the European Commission and supplemental obligations.

- Contractual right of Informatica to recover damages it can demonstrate it suffered as a result of the vendor's breach of the standard contractual clauses approved by the European Commission and supplemental obligations.

Organizational Measures

The Informatica Group may require of vendors:

- Commitment that the vendor will provide Informatica with notice if it becomes unable to comply with the standard contractual clauses approved by the European Commission without requirement to detail the reasons for such notice and that, if the vendor receives a request for any personal data from any government or law enforcement authority, the vendor will make commercially reasonable efforts to assert available defences against making the disclosure and will minimize the scope of any legally required disclosure to only that which is necessary to meet the disclosure obligation.

- Maintenance of data security and data privacy policies developed based on international standards (e.g., ISO certification).

Members of the Informatica Group may implement the following measures to protect data transferred to vendors:

- Conduction of risk assessments and vendor diligence to verify a vendor has appropriate technical and organizational safeguards in place before engaging the vendor, for example: the vendor's history of data security incidents, if the vendor executes ongoing risk assessments, tracks and has adequate contracts with sub-processors, maintains a code of business conduct, maintains processes for handling security and ransomware incidents, etc.

- Implementation of an ongoing priority-based compliance monitoring program for vendors, including regular audits for compliance with technical and organizational safeguards.

- Implementation of a law enforcement access policy to handle requests covering those that are redirected from vendors, including obligations (i) that it will thoroughly vet all law enforcement requests in accordance with Applicable Law; (ii) to challenge any request that, in Informatica's assessment, does not adhere to Applicable Law, and (iii) to reject any requests not subject to valid legal process (except in accordance with any predefined emergency-disclosure procedures the Informatica may have).