Version 2 2021-02-16

Itera

Data Protection Code

(Binding Corporate Rules for Processors)

Table of contents

1 Introduction

1.1 Applicability

This Data Protection Code applies to Itera ASA, Affiliates of Itera ASA and Private Entrepreneurs, jointly referred to as “the Itera Group” or "the Group". For the purpose of this Code, the term “Itera” refers to the whole Group or each of the members of the Group as the case may be.

The official list of the members of the Group bound by this Code is available on the company website. Itera Norge AS maintains and updates this list of the members of the Group when there is a change.

This Data Protection Code contains a set of legally binding rules within Itera, which provide principles for safeguarding Personal Data Processed by the Company Group on behalf of the Customers of the Group. The Data Protection Code, with associated policies, instructions and routines, constitutes the Binding Corporate Rules for Processors ("BCRP") for Itera.

The purpose of the Data Protection Code is to establish a legal basis for authorization of Transfer of Personal Data from Affiliates established within the EEA to Group members established outside the EEA (Third Countries, as defined below).

The Data Protection Code is part of Itera's Information Security Policy.

1.2 Data Protection

The Data Protection Code is based on the Norwegian Personal Data Act of 15 June 2018 no. 38 and the EU General Data Protection Regulation 2016/679 (GDPR). The GDPR does not allow for the Transfer of Personal Data to Third Countries that do not ensure an adequate level of data protection.

Itera is Processing Personal Data on behalf of Customers of the Group in its day-to-day business and regularly Transfers such Personal Data to its Affiliates, established both within and outside the EEA in accordance with contractual terms agreed with Customers.

Recognizing the importance of protection of Personal Data and legal requirements for Processing of Personal Data, as well as the strict rules regarding Transfers of Personal Data, Itera has committed to this Data Protection Code.

The Data Protection Code provides a legal basis for Data Protection Authorities in the EEA member states to authorise Transfers of Personal Data from Affiliates within the EEA to Group members in Third Countries. As a rule, Itera will be a Processor in accordance with Applicable Data Protection Law Processing Personal Data on behalf of the Customers. The Customers are as a general rule considered as Controllers in accordance with Applicable Data Protection Law deciding the means and purposes of the Processing.

1.3 Responsibility

Itera ASA is responsible for ensuring that the Data Protection Code is applied by all members of the Group.

This Data Protection Code is part of the Information Security Framework (IS Framework), and is as such under the responsibility of Itera's Group Data Protection Officer, cf. section 4.6.1. Each Local Data Protection Officer is responsible for the implementation of the Data Protection Code in its Affiliate/region. All employees, including Private Entrepreneurs, are responsible for adhering to this Code.

Within the authority limits in Itera, and subject to local laws and regulations, the Affiliates are responsible for all strategic and operational matters related to the day-to-day management of their business. It is the responsibility of the management of each Affiliate that the operations within the respective Affiliates are conducted in compliance with the Data Protection Code. This includes the responsibility for ensuring that internal control procedures are established, maintained and updated in case of deficiencies, as outlined in this Data Protection Code.

In a situation where a Data Subject lodges a complaint due to an alleged breach of the Data Protection Code, the concerned Affiliate shall without undue delay, take necessary steps to follow up the inquiry in accordance with the complaint mechanism referred to in section 4.7.

2 Description of Processing and Data flows

2.1 Itera as Processor and Customers as Controller

Itera is a provider of IT consulting services, including services related to operation, development, maintenance and testing. Itera provides its services to Customers primarily established in the Scandinavian Countries. In the course of providing such services to Customers, Itera regularly Processes Personal Data on behalf of Customers.

As a rule, each Customer will be the Controller deciding the means and purposes for the Processing, while Itera will be the Processor which processes data on behalf of the Customer.

2.2 Affiliates and Private Entrepreneurs bound by this Code

Itera has Affiliates established both within and outside the EEA, which are bound by this Code as part of Itera's Business Framework and by signing a written Agreement regarding bindingness with Itera ASA. The template "Agreement regarding bindingness – Affiliate" shall be used for this purpose.

Additionally, Itera has entered into long term agreements with a number of independent Private Entrepreneurs in Ukraine regarding IT consulting services, primarily regarding development and testing of IT-solutions on behalf of Itera. The Private Entrepreneurs works exclusively for Itera and all access to Personal Data on behalf of Itera's Customers takes place from Itera's premises in Ukraine by use of IT infrastructure provided by Itera. Private Entrepreneurs are obliged to comply with Itera's Business Framework and commit to comply with Itera's instructions. Private Entrepreneurs shall be explicitly bound by the obligations in this Code and is obliged to comply with all obligations pursuant to the Service Agreement and the Data Processing Agreement between Itera and the Customer. The template "Agreement regarding bindingness – Private Entrepreneurs" shall be used for this purpose.

Affiliates and Private Entrepreneurs shall Process Personal Data on behalf of Customers only on the basis of prior information to the relevant Customer and upon its prior written consent, cf. section 3.1.

2.3 Data exporters and importers

In accordance with the agreed project scope for each Customer Itera Transfers Personal Data back and forth between agreed Affiliates, Private Entrepreneurs and the relevant Customer on a regular basis.

Employees and Private Entrepreneurs will have access to Customers' systems from locations in Ukraine for agreed purposes.

The official list of the members of the Group bound by the BCRP is available on the company website.

2.4 Expected nature of Personal Data transferred and categories of Personal Data

This Data Protection Code applies to all Processing of Personal Data by Itera on behalf of Customers of the Group.

The nature of the Personal Data subject to Transfers will vary depending on the project scope agreed with the individual Customer, but will generally concern the following main categories:

- Identifying and indicative information (name, address, date of birth, telephone number, bank account number, personal id-number, photo etc.)
- Job information (title, position, working time, holidays, sick leaves and leave of absence information etc.)
- Compensation and benefits related information (gross salary, net salary, bonus etc.)

- Qualifications and performance information (competences, promotions etc.)
- Miscellaneous information (emergency contact, company benefit beneficiaries, contract details etc.)

For each new project, the scope of the Transfer will be defined.

2.5 Anticipated purposes for the Processing

The main purpose for Itera's Processing and Transfer of Personal Data will be to fulfil the contract with its Customers to provide them with the services requested. The anticipated Processing and Transfer will be related to the following basic activities:

- Design of systems and data model
- Analytics of data
- Development (development of new Customer IT-system or websites)
- Maintenance (maintenance of existing IT-systems or websites)
- Testing (testing of new IT-systems or websites prior to delivery or production)
- Operations and management of services, of data stored in Norway and Denmark (for internal Itera) and of customer data that resides with the customer at their chosen location, under their governance for access, processing and storage.

3 Contractual obligations and Customer's consent

3.1 Contractual obligations for Processing within the Group

This Code shall be made binding toward the Customer through a specific reference in the Service Agreement, cf. 4.3. As a Controller, each Customer has an obligation to sign a Data Processing Agreement, cf. GDPR Article 28, with Itera as Processor. A Data Processing Agreement template is made available on the Itera Intranet Site. Itera shall only Process Personal Data on behalf of the Customer (Controller) and under the instructions of the Customer as stated in the Service Agreement and the corresponding Data Processing Agreement.

Personal Data shall be subprocessed by Group Companies bound by the BCRP only with the prior informed specific or general written authorization of the Customer (Controller) in accordance with the Data Processing Agreement. The Data Processing Agreement will specify if a general prior authorization given at the beginning of the service would be sufficient or if a specific authorization will be required for each new subprocessing. If a general authorization is given, the Customer (Controller) should be informed on any intended changes concerning the addition or replacement of Internal Subprocessors in such a timely fashion that the Customer (Controller) has the possibility to object to the change or to terminate the contract before the data are communicated to the new Subprocessor. Changes to the list of potential Internal Subprocessors will be made available through the Itera website as mentioned in the BCRP section 2.2, see also section 4.10.

Subprocessing within the Group shall be governed by a separate subprocessing agreement on terms equivalent to the terms in the Data Processing Agreement with the Customer (Controller). The Customer (Controller) shall be provided with information about the main elements of the subprocessing, e.g. the parties and countries involved, security, guarantees in case of international transfers and information about the possibility to get a copy of the contracts used.

The Transfer of Personal Data within the Group is also subject to prior information to the Customer (Controller) and its prior written consent to such Transfers. Itera shall provide for transparency toward the Customer (Controller) and leave the Customer (Controller) in control of the Personal Data processed by Affiliates and Private Entrepreneurs on Customers (Controllers) behalf and under its instructions.

It shall be up to the Customer (Controller) to decide if this Code shall apply to:

- All Personal Data Processed for Processor activities and that are submitted to EU law; or
- All Processing of Personal Data Processed for Processor activities whatever the origin of the Personal Data.

During the performance of its tasks as Processor, Itera is obliged to process Personal Data in compliance with the obligations set out in the Service Agreement, the Data Processing Agreement and this Code.

3.2 Contractual obligations for Processing by use of External Subprocessors

Data may be subprocessed by External Subprocessors only with the prior informed specific or general written authorization of the Customer (Controller) in accordance with the Data Processing Agreement. The Customer (Controller) must be provided with information about the main elements of the sub-processing, e.g. the parties and countries involved, security, guarantees in case of international transfers and information about the possibility to get a copy of the contracts used. The detailed information, for example relating to the name of the subprocessors is provided in a public digital register.

If a general consent is given, the Customer (Controller) shall be informed on any intended changes concerning the addition or replacement of External Subprocessors in such a timely fashion that the Customer (Controller) has the possibility to object to the change or to terminate the contract before the Personal Data are communicated to the new Subprocessor.

Where the member of BCRP subcontracts its obligations under the Data Processing Agreement, with the authorization of the Customer (Controller), it shall do so only by way of a written agreement with the External Subprocessor which provides that adequate protection is provided as set out in Articles 28, 29, 32, 45, 46, and 47 of the GDPR. The written agreement shall further ensure that the External Subprocessor will have to respect the same obligations that are imposed on the member of the BCRP according to the Data Processing Agreement and provisions relevant for External Subprocessors in sections 4.3, 4.4, 4.8.1, 4.8.2, 4.9 and 5 of the BCRP. Particular emphasis shall be on providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR. The template “Example Subcontractor Data Processing Agreement” available on the Itera Intranet Site shall be used for these cases.

Transfers to External Subprocessors outside the EEA shall be carried out in compliance with the rules on Transfers in GDPR chapter V, e.g. by means of one of the following transfer mechanisms:

- EU Standard Contractual Clauses (Model Clauses 2010/87/EU); or
- External Subprocessor's Binding Corporate Rules for Processors.

If EU's Contractual Clauses (Model Clauses 2010/87/EU) are used, the non-EEA-based External Subprocessor shall be “data importer” and the EEA-based Customer of Itera shall be “data exporter”. Customers and the External Subprocessors may sign the Model Clauses directly, or the Customer may give one (or more) EEA-based Affiliates of Itera a clear mandate to sign the Model Clauses with any non-EEA-based External Subprocessor in the name and on behalf of the Customer.

4 Key principles of the Data Protection Code

4.1 Accountability

The Group has a duty to make available to Customers acting as Controllers all information necessary to demonstrate compliance with their obligations as provided by GDPR Article 28(3)(h) and allow for and contribute to audits, including inspections conducted by the Controller or another auditor mandated by the Controller. In addition, Itera shall inform the Controller within a reasonable time period if in its opinion, an instruction infringes Applicable Data Protection Law.

The Group Companies need to maintain a record of all categories of processing activities carried out on behalf of each Customer acting as Controller in line with the requirements as set out in GDPR Article 30(2). The record will be maintained and be made available to the competent Data Protection Authority on request.

Members of the Group shall assist the Customer acting as Controller in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate compliance with the requirements set up by the BCRP in practice, such as data protection by design and by default on provided services.

4.2 The duty to respect the BCRP

The Group’s commitment to comply with this Code including instructions regarding the Processing of Personal Data and the security and confidentiality measures as provided in the Service Agreement and the Data Processing Agreement is established by each Affiliate and Private Entrepreneurs signing an Agreement regarding bindingness with regard to Itera’s Data Protection Code (BCRP).

Each Itera employee is bound by the rules in this Code, including the instructions regarding the Processing of Personal Data and the security and confidentiality measures as provided in the Service Agreement and the Data Processing Agreement. This is achieved by way of specific obligations contained in each contract of employment signed by the employees, as well as in Itera's Information Security Framework and by linking observance of this Code with disciplinary procedures and sanctions, cf. section 4.5.

4.3 Binding toward the Controller

The BCRP is made binding toward the Customers acting as Controllers through a specific reference in the Customer Service Agreement and the Data Processing Agreement pursuant to GDPR Article 28. Hence, the Customer Service Agreement and the Data Processing Agreement will ensure that the Group is bound by the BCRP towards the Customers as Controllers. The BCRP will be annexed to the Service Agreement or a reference will be made to an electronic version of the BCRP, cf. section 4.4.2.

All Customers (Controllers) shall have the right to enforce the BCRP against any member of the Group for their breaches of the Code.

Moreover, all Customers (Controllers) shall have the right to enforce the BCRP against Itera ASA for breaches of the BCRP caused by any Itera Affiliate established outside the EEA.

Finally, all Customers (Controllers) shall have the right to enforce the BCRP against Itera ASA for breaches of the BCRP caused by External Subprocessors established outside of EU/EEA.

Where a Customer (Controller) can demonstrate that they have suffered damage and establish facts that show that it is likely that the damage has occurred due to breach of the BCRP, it will be for Itera ASA to prove that the member of the Group, or the External Subprocessor outside of the EEA, was not responsible for the breach of the BCRP, giving rise to those damages or that no such breach took place.

To the extent permitted by applicable law, the compensation for damages shall be limited to direct damages which exclude, without limitation, lost profits or revenue, lost turnover, cost of capital and downtime cost.

Where Itera ASA can prove that any member of the Group or the External Subprocessor outside the EEA is not responsible for the breach of the BCRP, it may discharge itself from any responsibility toward the Customer (Controller).

4.4 Data Subjects’ and Controllers' rights

4.4.1 Data Subjects' beneficiary rights

The BCRP grant rights to Data Subjects to enforce the BCRP as third-party beneficiaries directly against the Group with regard to requirements that are specifically directed to Processors in accordance with the GDPR. In this regard, Data Subjects shall be able to enforce the following elements of the BCRP directly against the Group:

- The duty to respect the instructions from the Customer acting as Controller regarding the data Processing, including for transfers to Third Countries;
- The duty to implement appropriate technical and organizational security measures and the duty to notify any Personal Data Breach to the Customer acting as Controller;
- The duty to respect the conditions when engaging a Subprocessor either within or outside the Group;
- The duty to cooperate with and assist the Customer acting as Controller in complying and demonstrating compliance with Applicable Data Protection Law such as for answering requests from Data Subjects in relation to their rights;
- The right to information and easy access to the BCRP;
- The right to complain through the Complaint Handling Process (cf. the Code section 4.7);
- The duty to cooperate with the Data Protection Authorities;
- The liability, compensation and jurisdiction provisions; and
- The need to be transparent where national legislation prevents the Group from complying with the BCRP.

The beneficiary rights granted to Data Subjects according to this BCRP is subject to the Data Subject not being able to bring a claim against the Customer because the Controller has factually disappeared or ceased to exist in law or has become insolvent. However, this does not apply if any successor entity has assumed the entire legal obligations of the Customer (Controller) by contract or by operation of law, in which case the Data Subject can enforce its rights against such successor entity.

The Data Subject’s third-party beneficiary rights include the right to enforce:

- The duty to respect the BCRP (cf. the Code section 1.1, 3 and 4.5);
- The possibility to lodge a complaint before the competent Data Protection Authorities and before the courts (cf. this section 4.4.1);
- Liability in accordance with section 4.4.3 of this BCRP;
- The burden of proof that lies with the company not the individual (cf. the Code section 4.4.3);
- The right to information and easy access to the BCRP (cf. the Code section 4.4.2.);

- The existence of a complaint procedure (cf. the Code section 4.7);
- The duty to cooperate with the Data Protection Authorities (cf. the Code section 4.8.1);
- The duty to cooperate with the Customer acting as Controller (cf. the Code section 4.8.2);
- The Privacy Principles including the rules on Transfers or onward Transfers out of the EEA (cf. the Code section 5);
- The list of the entities bound by the BCRP, their location and contact details; and
- The need to be transparent where national legislation prevents the Group from complying with the BCRP (cf. the Code section 4.9).

The Data Subjects rights mentioned above shall cover the judicial remedies for any breach of the third party beneficiary rights guaranteed and the right to obtain redress and where appropriate receive compensation for any damage (material harm but also any distress).

Data Subjects shall be entitled to lodge a complaint before:

- the Data Protection Authority of the EEA Member State of the Data Subject's habitual residence, place of work or place of alleged infringement; or
- the competent court of the EEA Member State where the Controller or Processor has an establishment or where the Data Subject has his or her habitual residence pursuant to GDPR Article 79.

Where Itera and the Customer acting as the Controller involved in the same Processing are found responsible for any damage caused by such Processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from Itera acting as the Processor, cf. GDPR Article 82(4).

4.4.2 Information

All Data Subjects who benefit from the Data Protection Code shall have easy access to information describing their rights.

This Data Protection Code (BCRP) shall be published and be publically available online on Itera's website. The public version shall constitute the entire Itera Binding Corporate Rules (BCRP) applicable for the Processing of Personal Data on behalf of Customers of the Group, including the third party beneficiary rights cf. section 4.4.1.

Additionally, Itera's Code of Conduct published on Itera's website will provide supplementary information on Itera's activities in Ukraine.

4.4.3 Liability

Itera has appointed Itera ASA to take on the responsibility for any damages resulting from the violation of the Data Protection Code by the Group and External Subprocessors. Itera ASA takes on the responsibility of taking necessary action to remedy the acts of other members of the Group established outside of the EEA or breaches caused by External Subcontractors established outside of the EEA and, where appropriate, to pay compensation for any damages resulting from violation of the Data Protection Code.

Itera ASA accepts liability as if the violation has taken place by Itera ASA in Norway instead of the member of the Group outside the EEA or the external Subcontractor established outside the EEA. Itera ASA may not rely on breach by a Subcontractor (internal or external of the Group) of its obligations in order to avoid its own liabilities.

Where a Data Subject, or Controller, can demonstrate that they have suffered damage and establish facts that show that it is likely that the damage has occurred due to breach of the Code. Then it will be for Itera ASA to prove that the member of the Group, or the external Subcontractor outside of the EEA, was not responsible for the breach of the Code, giving rise to those damages or that no such breach took place.

Where Itera ASA can prove that any member of the Group or External Subcontractor, outside the EEA, is not responsible for the breach of the BCRP, it may discharge itself from any responsibility toward the Data Subject.

4.5 Effective compliance

Itera has established several measures, as further described below, which guarantees implementation and compliance with the Data Protection Code among Itera's employees and Private Entrepreneurs who either:

- have permanent or regular access to Personal Data;
- are involved in the collection of Personal Data; or
- are involved in the development of tools or applications used to process Personal Data.

Observance of the Data Protection Code shall be linked with disciplinary procedures.

4.5.1 The Code as part of Itera's Business Framework structure

The issuing of this Data Protection Code as part of Itera's Business Framework is an important measure in the process of achieving sufficient data privacy safeguards amongst all employees.

4.5.2 Contracts of employment

Itera's contracts of employment shall include specific obligations for all employees to adhere to this Data Protection Code.

4.5.3 Information Security Framework (IS Framework)

Itera has implemented a specific chapter in Itera's Information Security Framework (IS Framework) regarding obligations to comply with Itera's Data Protection Code. The IS Framework is part of Itera's Business Framework and is binding upon employees and Private Entrepreneurs.

4.5.4 Introduction courses

All new employees, including Private Entrepreneurs, shall complete a mandatory introduction program regarding the rules in this Code. All new employees at Itera, including Private Entrepreneurs, will go through a training during the introduction day to ensure knowledge building and to ensure that Itera follow the principles in the Data Protection Code. This introduction day occurs monthly in the Itera group. There will also be attached a sign-off to the contract to confirm that the employee is tested on sufficient knowledge of the Data Protection Code to be signed on the introduction day. For External Subprocessors, each resource manager at Itera responsible for the External Subprocessor will provide relevant information regarding the BCRP.

4.5.5 Awareness and training

All employees and Private Entrepreneurs, shall at all times have access to the Data Protection Code at the IS Framework on the Itera Intranet Site. In addition, information shall be presented via relevant communication channels to ensure awareness among all employees of individual rights and duties concerning the Code.

Itera provides a mandatory e-learning course available on the Itera Intranet Site. The course is mandatory and includes several modules explaining the principles set out in the Data Protection Code and provides practical guidance for the Prosessing of Personal Data. The mandatory e-learning training program will be combined with reccuring information sessions.

Additionally, Itera will provide a mandatory and elaborate e-learning training program for personnel, including Private Entrepreneurs, who

- have permanent or regular access to Personal Data;
- are involved in the collection of Personal Data; or
- are involved in the development of tools or applications used to process Personal Data.

Further, information and use of the Data Protection Code will be part of the management training through Itera Academy.

It will be the department managers' responsibility that all employees have attended and successfully completed the courses mentioned above.

The Group Data Protection Officer, in cooperation with the Local Data Protection Officers, shall be responsible for providing the relevant information and setting up/updating the mandatory e-learning training programs described above.

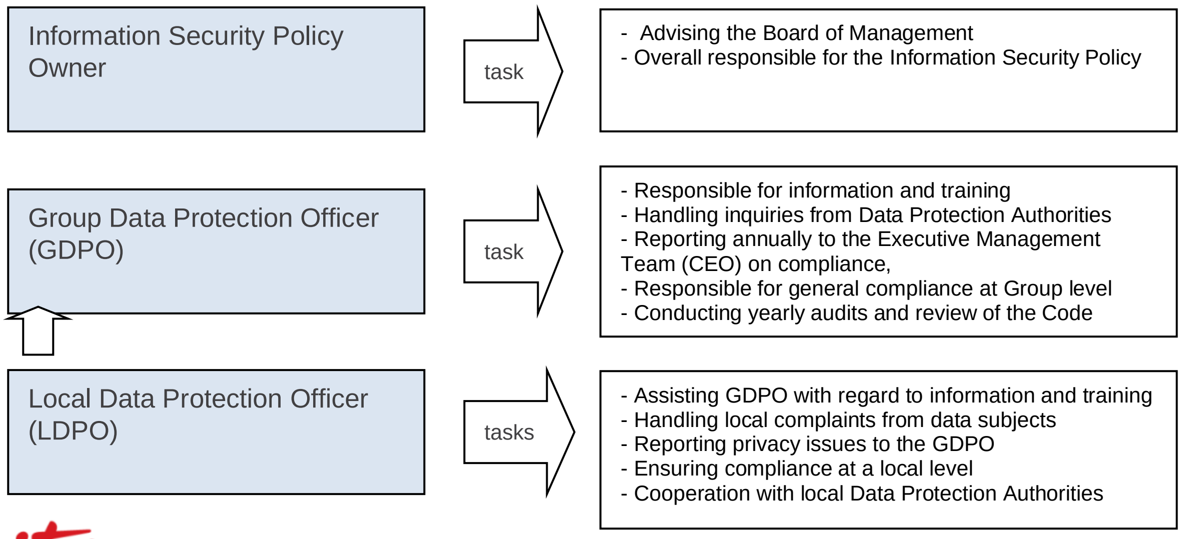
4.6 Supervision and audit

The Data Protection Code has several measures to ensure compliance and supervision of compliance. This includes:

- The appointment of one Group Data Protection Officer in accordance with GDPR Article 37;
- The appointment of one Local Data Protection Officer for each Affiliate and/or Region;
- Establishment of internal control mechanisms to ensure ongoing monitoring; and
- Establishment of an audit and review program.

4.6.1 Policy owner and Data Protection Officers

Itera has appointed the following positions to oversee and ensure compliance with the rules of this Data Protection Code:



Information Security Policy Owner

- Advising the Board of Management
- Overall responsible for the Information Security Policy

Group Data Protection Officer (GDPO)

- Responsible for information and training
- Handling inquiries from Data Protection Authorities
- Reporting annually to the Executive Management Team (CEO) on compliance,
- Responsible for general compliance at Group level
- Conducting yearly audits and review of the Code

Local Data Protection Officer (LDPO)

- Assisting GDPO with regard to information and training
- Handling local complaints from data subjects
- Reporting privacy issues to the GDPO
- Ensuring compliance at a local level
- Cooperation with local Data Protection Authorities

The Group Data Protection Officer is granted an appropriate level of independency in the exercise of his functions.

The Group Data Protection Officer and the Local Data Protection Officers shall be the main contact point between relevant Data Protection Authorities and Itera on any matter arising out of the Code or Processing of Personal Data in general. If such Data Protection Officer is not appointed locally, the main contact person locally shall be the CEO of the relevant Affiliate together with the Group Data Protection Officer.

Further description of the Group Data Protection Officer and Local Data Protection Officers' responsibilities is set out in Guidelines for Data Protection Officers.

4.6.2 Internal control and ongoing monitoring

Affiliates in Itera shall structure their internal control systems to monitor themselves on an ongoing basis. The monitoring procedures for this Data Protection Code shall be built into the normal, recurring operating activities for each Affiliate, as stated in Itera's Business Framework.

4.6.3 Audit and review program

To ensure enforcement of the Data Protection Code, Itera shall ensure that an audit of the Code take place each year, in accordance with Itera's Data Protection Compliance Review Plan.

The Compliance Review Plan shall cover all aspects of the BCRP including methods to ensure that corrective actions are implemented. The result of audits will be communicated to the Group Data Protection Officer and to the ultimate parent's board and will also be made accessible to the relevant customers upon request. Additionally, the competent Data Protection Authorities shall have access to the results of the audit upon request and shall have the authority to carry out a data protection audit if required and legally possible.

Itera shall ensure that any Processor or any Subprocessor handling data on behalf of a particular Customer (Controller) accepts at the request of that Customer, to submit for audit their data processing facilities used for Processing of Personal Data on behalf of the Customer. The audit can be conducted by the Customer or an inspection body composed of independent members in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Controller, where applicable, in agreement with the competent Data Protection Authority.

4.7 Complaint mechanisms

All Data Subjects, who benefit from rights according to this Code cf. section 4.3, shall have the right to claim that any of Itera’s Affiliates is not compliant with the Data Protection Code, by lodging a complaint.

Data subjects may file a complaint by contacting the Group Data Protection Officer, either by clicking the link on Itera's web site www.itera.no, by sending an email to dpo@itera.no, or regular mailto Itera ASA, Postboks 4841 Nydalen, 0422 Oslo, Norway.

Any member of the Group shall have a duty to without delay communicate a claim or request from a Data Subject to their Local Data Protection Officer. The Local Data Protection Officer, in collaboration with the Group Data Protection Officer, shall assess whether the claim or request shall be communicated to the Customer within reasonable timeframe, or whether the claim or request shall be handled internally by Itera, e.g. because:

- It has been agreed with the Customer that claims and request shall be handled by Itera; or
- The data subject has a right to lodge a complaint because the Customer has factually disappeared, has ceased to exist in law or has become insolvent except, unless any successor entity has assumed the entire legal obligations of the Customer by contract or by operation of law, cf. section 4.4.1.

Data Subjects' queries and complaints that according to the above shall be handled internally by Itera, shall be handled without undue delay by the relevant Local or Group Data Protection Officer and in any event within one month. Considering the complexity and number of requests, that period may be extended by two further months, in which case the Data Subject should be informed accordingly.

In case the complaint is considered as justified Itera shall take necessary steps to resolve the matter and implement corrective measures to ensure compliance with the Code and Applicable Data Protection Law.

In case of rejection of the complaint the Data Subject shall be given an explanation of the reason for the rejection.

If the Data Subject is not satisfied with Itera's complaint handling the Data Subject shall be entitled to lodge a claim before the Court or the relevant Data Protection Authority.

4.8 Mutual assistance and cooperation with Data Protection Authorities

4.8.1 Duty to cooperate with Data Protection Authorities

All members of the Group undertake to cooperate with the Data Protection Authorities competent for the relevant Customer (Controller), particularly with respect to:

- Accept to be audited by the relevant Data Protection Authority; and
- Comply with the advice the Data Protection Authorities on any issues relating to the BCRP.

4.8.2 Duty to cooperate with Controller

All members of the Group and External Subprocessors shall, within a reasonable time, and to the extent reasonably possible, cooperate with and assist the EEA Customer (Controller) to comply with Applicable Data Protection Law.

4.9 Relationship between national laws and the Data Protection Code

The Data Protection Code is based on the EU General Data Protection Regulation 2016/679 and the Norwegian Personal Data Act of 15 June 2018 no.38. The purpose of the Data Protection Code is to ensure compliance with this legislation, and to ensure adequate safeguards for the Transfers of Personal Data. However, the Data Protection Code should not be considered as an instrument to replace relevant and mandatory data protection laws.

The Data Protection Code will not take precedence over local legislation when local legislation provides a higher level of protection for Personal Data. Hence, Data Subjects keep any rights and remedies they may have under applicable local law. This Code shall apply only where it provides supplemental protection for Personal Data. Where applicable local law provides a higher level of protection than this Code, local law shall take precedence over the BCRP.

If Itera has reasons to believe that applicable existing or future legislation prevents the fulfilling of obligations under the rules of this Data Protection Code or the Service Agreement and corresponding Data Protection Agreement, Itera has an obligation to promptly inform the Customer acting as Controller. In that case, the Customer is entitled to suspend the Transfer of Personal Data and/or terminate the Service Agreement with Itera. Sufficient information shall be provided to Itera or to the Data Protection Officer and to the Data Protection Authority competent for the Customer acting as Controller and the lead Data Protection Authority for the BCRP.

Any legally binding request for disclosure of Personal Data by a law enforcement authority or state security body shall be communicated to the Controller unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. In any case, the request for disclosure should be put on hold and the Data Protection Authority competent for the Controller and the lead Data Protection Authority for the BCRP shall be clearly informed about the request, including information about the data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited).

If notifications as set out above is prohibited, the Affiliate shall use its best efforts to obtain the right to waive the prohibition in order to communicate as much information as it can and as soon as possible. The Affiliate shall document its efforts.

If the Affiliate, despite having used its best efforts, is not able to notify the competent Data Protection Authorities, the Affiliate shall provide general information on the requests it received to the competent Data Protection Authorities (e.g. number of applications for disclosure, type of data requested, requester, etc.).

4.10 Procedure for updating the Data Protection Code

Itera may make amendments to the Code, e.g. to take into account amendments in the regulatory environment or changes to Itera's corporate structure. Such amendments or changes shall be reported to all Group members, to the Data Protection Authorities and the Customers (Controllers).

If a change of the Code affects the Processing conditions, relevant information shall be provided to the Customer in such a timely fashion that the Customer has the possibility to object to the change or to terminate the Service Agreement with Itera before the modification is made (for instance, on any intended changes concerning the addition or replacement of Subprocessors, before the data are communicated to the new Subprocessor).

Updates of the Code are possible without having to re-apply for authorization by the Data Protection Authorities, provided that:

a) The Group Data Protection Officer keeps a fully updated list of Group members and Subcontractors involved in the Personal Data Processing activities for the Customer which shall be accessible for the Controller, Data Subject and Data Protection Authorities;
b) The Group Data Protection Officer keeps track of and record of any updates to the rules and provide the necessary information systematically to the Customer and upon request to Data Protection Authorities;
c) No Transfer of Personal Data is made to a new member until the new member is effectively bound by this Data Protection Code, and can demonstrate compliance;
d) Any changes to the Code or to the list of members shall be reported once a year to the lead Data Protection Authoritiy with a brief explanation of the reason justifying the update. Where a modification would affect the level of protection offered by the BCRP or significantly affect the BCRP (i.e. changes in the bindingness), it must be promptly communicated to the Norwegian Data Protection Authority.

5 General privacy principles observed by Itera

Itera and External Subprocessors of Itera Processing Personal Data on behalf of Customers of Itera shall assist the Customers in their role as Controllers with regard to adhering to the following data protection principles in the EU General Data Protection Regulation 2016/679.

5.1 Transparency, fairness and lawfulness

Itera and External Subprocessors of Itera shall help and assist the Customer (Controller) to comply with applicable requirements with regard to fair, transparent and lawful Processing. Itera shall provide the Customer (Controller) with necessary information to allow the Customer (Controller) to comply with information requirements toward Data Subjects.

5.2 Purpose limitation

Itera and External Subprocessors of Itera shall process Personal Data only on behalf of the Customer (Controller) and in compliance with the Customer's (Controller's) instructions, including with regard to Transfers to a Third Country, unless required to do so by Applicable Data Protection Law to which Itera is subject. In such a case, Itera shall inform the Customer (Controller) of that legal requirement before Processing takes place, unless the law prohibits such information on important grounds of public interest.

In other cases, if Itera cannot provide such compliance for whatever reasons, Itera agrees to inform promptly the Customer (Controller) of its inability to comply, in which case the Controller shall be entitled to suspend the Transfer of data and/or terminate the relevant service.

On the termination of the provision of data processing services for a Controller, Itera and any Subprocessor of Itera shall, at the choice of the Customer (Controller), delete or return all the Personal Data transferred and the copies thereof to the Customer (Controller) and delete the copies thereof. Itera and any Subprocessor must certify to the Customer (Controller) that it has done so, unless legislation imposed upon them requires storage of the Personal Data transferred. This prevents returning or destroying all or part of the Personal Data transferred. In that case, Itera and the Subprocessors will inform the Customer (Controller) and warrant that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

5.3 Data quality and proportionality

Itera and External Subprocessors of Itera shall have a general duty to help and assist the Customer (Controller) in complying with Applicable Data Protection Law. This includes in particular a duty to:

- Execute any necessary measures when asked by the Customer (Controller), in order to have the Personal Data updated, corrected or deleted;
- Inform each member of the Group and/or External Subprocessors to whom the data have been disclosed of any rectification, or deletion of data;
- Execute any necessary measures, when asked by the Customer (Controller), in order to have the data deleted or anonymised from the moment the identification form is not necessary anymore;
- Communicate to each entity to whom the data have been disclosed and of any deletion or anonymization of data.

5.4 Security

Itera and Subprocessors of Itera have the following duties with regard to security:

- Implement all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the Processing as provided by GDPR Article 32;
- Assist the Customer (Controller) in ensuring compliance with the obligations as set out in GDPR Articles 32 to 36, taking into account the nature of Processing and information available to the Processor;
- Inform the Customer (Controller) without undue delay after becoming aware of any Personal Data Breach;

In addition, Subprocessors shall have the duty to inform Itera and the Customer (Controller) without undue delay after becoming aware of any Personal Data Breach.

5.5 Data Subject's rights

Itera and External Subprocessors of Itera will execute any necessary technical and organizational measures when asked by the Customer (Controller) insofar as this is possible, for the fulfilment of the Customer's (Controller's) obligations to respond to requests for exercising Data Subjects' rights as set out in GDPR Chapter III. This includes communicating any useful information in order to help the Customer (Controller) to comply with the duty to respect the rights of the Data Subjects. Itera and External Subprocessors of Itera will transmit to the Controller any Data Subject's request without answering it unless he is authorised to do so.

6 List of definitions

6.1 Applicable Data Protection Law

The EU General Data Protection Regulation 2016/679 (GDRP) and any national data protection laws and regulations applicable to Itera in the role as Processor under the BCRP.

6.2 Affiliate

Any subsidiary of which Itera ASA directly or indirectly owns at least 50 % of the voting interest and which is governed by the Itera's Business Framework.

6.3 Binding Corporate Rules for Processors (BCRP)

A set of personal data protection policies which are adhered to by a Processor established in the territory of an EU or EFTA-member state for transfers or a set of transfers of Personal Data to a Controller or Processor in one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

6.4 Controller

A Customer of Itera which alone or jointly with others determines the purposes and means for the Processing of Personal Data and on whose behalf Itera Processes Personal Data.

6.5 Customer

Any natural or legal person having engaged Itera as a provider of IT-solutions and related services and being the Controller deciding the means and purposes for the Processing of Personal Data, cf. the definition of Controller.

6.6 Data Protection Officer

A natural person holding a position within Itera to oversee and ensure compliance and supervision of compliance of the Data Protection Code in accordance with GDPR Articles 37-39.

6.7 Data Subject

An identified or identifiable individual to whom the Personal Data being processed relates.

6.8 EEA

The European Economic Area, meaning the EU member states together with the EFTA countries (Liechtenstein, Iceland and Norway).

6.9 External Subprocessor

Any natural or legal person which is not part of the Group to whom a member of the Group has subcontracted its obligations under the Service Agreement and the Data Protection Agreement with the Customer by way of written agreement and which processes the Personal Data on behalf of the Controller, cf. section 3.2.

6.10 Internal Subprocessor

Any natural or legal person which is part of the Group to whom a member of the Group has subcontracted its obligations under the Service Agreement and Data Protection Agreement with the Customer in accordance with section 3.1.

6.11 Itera Group (Group)

Itera ASA, Affiliates and Private Entrepreneurs bound by this BCRP are jointly referred to as "the Itera Group" or "the Group", cf. section 1.1. For the purpose of this Code, the term “Itera” refers to the Itera Group or each of the Affiliates or Private Entrepreneurs as the case may be.

6.12 Personal Data

Personal data shall mean any information that may be related to an identified or identifiable individual (the “Data Subject”).

An identifiable individual is a person who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Personal Data includes all types of information that directly or indirectly may be linked to the Data Subject. Personal data may include:

- Names and dates of birth;
- Contact details such as addresses, e-mail addresses and telephone numbers;
- Indirect information such as IP address, laptop name etc.;
- Expressions of opinions on living individuals; or
- Information concerning salary, job qualifications, health etc.

6.13 Private Entrepreneurs

Any natural person registered as Private Entrepreneur according to the Ukrainian Unified State Register of Legal Entities and Private Entrepreneurs, who have entered into a "Private Entrepreneur Agreement" with Itera Offshoring Services AS regarding consulting service in the area of information technology and being part of this BCRP on the basis of an "Agreement regarding bindingness", whereby the Private Entrepreneur has accepted to comply with the BCRP and to comply with the BCRP's third party beneficiary rights.

6.14 Processing

Any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, alignment, storage and disclosure, or a combination of such use. The definition is technology-neutral and includes the Processing of Personal Data that is wholly or partly performed with the aid of computers or similar equipment that is capable of automatically Processing Personal Data. The definition also includes manual registers or filing systems if the Personal Data is included in, or is intended to form part of, a structured collection making the Personal Data available for searching or compilation according to specific criteria.

6.15 Processor

Any natural or legal person who Processes the Personal Data on behalf of the Controller, for example an Affiliate or Private Entrepreneur.

6.16 Special Categories of Personal Data

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.

6.17 Third Countries

Countries outside the European Economic Area (EEA), i.e. all countries except the EU member states and the EFTA member states (Liechtenstein, Iceland and Norway).

6.18 Transfer

Any Personal Data disclosure, copy or move via a network, access from a system or web application or any Personal Data disclosure, copy or move from one medium to another irrespective of type of medium from the EEA to a recipient outside the EEA (Third Country).