ICL Services General Personal Data Protection Policy

Document reference:	POL-IS-18
Version:	1.0
Status:	Approved
Last revision:	08.11.2019
Owner:	Ruslan Vagizov
Authorized by:	Ruslan Vagizov

Table of contents

1. Purpose, Scope and Users

GDC Services LLC, hereinafter also referred to as the “ICL Services” or “Company”, strives to comply with applicable laws and regulations related to Personal Data protection in countries where the Company operates and its Customers operate. This Policy sets forth the basic principles by which the Company processes the personal data of consumers, customers, suppliers, business partners and other individuals on behalf of Data Controllers and Data Processors within European Economic Area (EEA), and indicates the responsibilities of its business departments and employees while processing personal data in the provision of IT services for EEA customers.

This Policy is developed in accordance with the requirements of the Regulation No. 2016/679 of the European Parliament and of the Council of the European Union "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data" (General Data Protection Regulation, hereinafter - GDPR).

This Policy applies to the Company and its associated companies, which directly or indirectly control or are controlled by the Company (including but not limited to ICL Services and Solutions d.o.o, Belgrade) providing the services within EEA or processing the personal data of data subjects within EEA.

With regard to the processing of personal data of consumers, employees, customers, suppliers, business partners, and other individuals, collected on the territory of Russian Federation and other countries, non-EU members, the Company is guided by the federal law of the Russian Federation on personal data (152-FZ) and relevant data protection laws of these countires.

This document applies to all employees, permanent and temporary, and all contractors working on behalf of The Company.

This Policy is a publicly available document and must be posted on the official website of the Company.

2. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union’s General Data Protection Regulation:

Personal Data: Any information relating to an identified or identifiable natural person ("**Data Subject**") 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.

Sensitive Personal Data: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing: An 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 of the data.

Data Processing Agreement: This is a general definition of any agreement between the Company and Data Controllers or other Data Processors in the supply chain that governs the processing and protection of personal data (for example, Data Transfer Agreement, Data Processing Agreement, Data Protection Appendix to Master Service Agreement etc.).

Anonymization: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymization: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymization reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymized data is still personal data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

Cross-border processing of personal data: Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

"Main establishment as regards a controller" with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

Group Undertaking: Any holding company together with its subsidiary.

3. Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for organisations handling personal data. Article 5 of the GDPR stipulates that:

1. *Personal data shall be:*
    - *processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');*
    - *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation**');*
    - *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');*
    - *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');*

- *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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘**storage limitation**’);*
- *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality’**).*

2. *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘**accountability**’*).

Article 28(1) the GDPR stipulates that: “*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”*

The Company recognizes and respects the abovementioned principles of personal data processing and assumes the following obligations:

- provide all possible assistance to data controllers in compliance with these principles and demonstrate compliance.
- implement appropriate technical and organisational measures (in the Company’s area of control) in such a manner that processing meets the requirements of this Regulation and ensure the protection of the rights of the data subject.

Requirements for the necessary volume of assistance, as well as appropriate technical and organisational measures to be implemented by the Company, should be clearly stated in Data Processing Agreements with data controllers or other data processors from which these personal data are obtained.

4. Building Data Protection in Business Activities

In order to demonstrate compliance with the principles of data protection, the Company should build data protection into their business activities.

4.1 Notification to Data Subjects

At the time of collection or before collecting personal data for any kind of processing activities including but not limited to selling products, services, or marketing activities, data controller is responsible to properly inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and the data controller's security measures to protect personal data.

The Company does not collect any personal data of data subjects within EEA on its own. Notification to data subjects is the responsibility of data controller that transmits the processing of personal data to the Company or to any other data processor in the supply chain.

4.2 Data Subject's Choice and Consent

Whenever personal data processing is based on the data subject's consent, or other lawful grounds, data controller is responsible for retaining a record of such consent. Data controller is responsible for providing data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

The Company does not collect any personal data of data subjects within EEA on its own. Obtaining consent from data subjects is the responsibility of data controller that transmits the processing of personal data to the Company or to any other data processor in the supply chain.

4.3 Collection

Data controllers should strive to collect the least amount of personal data possible.

The Company does not collect any personal data of data subjects within EEA on its own.

All categories of personal data that the Company receives for processing should be specified in the relevant agreements with data controllers or other data processors from which these personal data are obtained. These agreements should provide for the obligation of the transferring party to ensure that the personal data is collected lawfully.

Data Protection Consultant (The role of a Data Protection Consultant is distribute in paragraph 5 of this Policy) must ensure that categories of personal data and obligations of the transferring party are specified in the data processing agreements.

4.4 Use, Retention, and Disposal

The purposes, methods, storage limitation and retention period of personal data must be consistent with the Notification to data subjects. Data controllers must maintain the accuracy, integrity, confidentiality and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data must be used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches.

The Company undertakes to strictly follow the instructions of data controllers related to the use, retention, and disposal of personal data, and ensure adequate security mechanisms in accordance with data processing agreements with data controllers or other data processors in the supply chain.

Data Protection Consultant must ensure that instructions from the data controllers are received and adequate security mechanisms are described in the data processing agreements.

4.5 Disclosure to Third Parties

Whenever the Company uses a third-party supplier or business partner to process personal data on its behalf, Data Protection Consultant must ensure that this processor provides security measures to safeguard personal data that are appropriate to the associated risks. For this purpose, the Processor's GDPR Compliance Questionnaire must be used.

The Company must contractually require the supplier or business partner to provide the same level of data protection. The supplier or business partner must only process personal data to carry out its contractual obligations towards the Company or upon the instructions of the Company or direct data controller's instructions and not for any other purposes. When the Company processes personal data jointly with an independent third party, the Company must explicitly specify its own respective responsibilities and of the third party in the relevant Data Processing Agreement with the Supplier.

4.6 Cross-border Transfer of Personal Data

Before transferring personal data out of the European Economic Area (EEA) adequate safeguards must be used by the Controller, including the signing of a Data Transfer Agreement based on the Standard Contractual Clauses (Model Clauses), as required by the European Union and, if required, authorization from the relevant Data Protection Authority must be obtained.

The Company is a data processor and undertakes the fulfillment of all applicable requirements specified by EEA data controllers in their Data Transfer Agreements with the Company.

If the Company intends to carry out further cross-border transfer of data processing, the Company will obtain consent for such a transfer from the data controllers or other data processors in the supply chain and will require the entity importing the personal data to comply with the principles of personal data processing set forth in the Company's Cross Border Data Transfer Procedure.

4.7 Rights of Access by Data Subjects

Data controllers are responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law.

The Company as a data processor will support and assist data controllers with respect to their obligations related to execution of and providing information on Personal Data subject rights in accordance with the Data Controller Request Procedure and data processing agreements with data controllers or other data processors in the supply chain.

4.8 Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to data controllers in a structured format and to transmit those data to another controller, for free. Data controllers are responsible to ensure that such requests are processed without undue delay, are not excessive and do not affect the rights to personal data of other individuals.

The Company as a data processor will support and assist data controllers with respect to their obligations related to data portability in accordance with the Data Controller Request Procedure and data processing agreements with data controllers or other data processors in the supply chain.

4.9 Right to be Forgotten

Upon request, Data Subjects have the right to obtain from data controllers the erasure of their personal data. Data Controller must take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

The Company as a data processor will support and assist data controllers with respect to their obligations related to execution of Data Subjects right to be forgotten in accordance with the Data Controller Request Procedure and data processing agreements with data controllers or other data processors in the supply chain.

5. Contact regarding the processing of personal data

Data Protection Consultant is responsible in the Company for managing the personal data protection program and for the development and promotion of end-to-end personal data protection policies. Data Protection Consultant accepts any questions or suggestions regarding the processing of personal data. You can contact Data Protection Consultant at the e-mail address privacy@icl-services.com .

6. Response to Personal Data Breach Incidents

When the Company becomes aware of a suspected or actual personal data breach, Data Protection Consultant must perform an internal investigation and take appropriate remedial measures in a timely manner, according to the Security Incident Management Process and the special Procedure for Personal Data Breach. The Company must notify the relevant data controller about any accidental, unauthorised access, or other personal data breach without undue delay and, when possible, within 24 hours.

7. Audit and Accountability

The Internal Audit Group is responsible for auditing compliance of the Company's departments with this Policy.

The Company grants data controllers and other data processors upstream in the supply chain the control and examination rights. These rights include:

- the right to obtain information from the Company on the implementation and execution of the obligations set forth in data processing agreements, including inspection of the relevant documentation demonstrating compliance with this data processing agreements and Data Protection Legislation;
- the right to appoint internal or independent auditor to inspect Company's compliance with the data processing agreements and Data Protection Legislation.
- the right of to obtain information on agreements with sub-processors downstream of the supply chain.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations of the Russian Federation.