

Personal data handling according to GDPR

January of 2019

The principles how UAB Softera Baltic (reg. no. 301566552) processes personal data are described in these **Personal data handling according to GDPR**, hereinafter also referred as the **principles**.

The principles apply if the Client uses, has used or has expressed an intention to use or is in other way related to any of the services provided by the Company, including to the relationship with the Client established before these principles entered into force.

1. Definition

Client means a legal entity whose registered office is <address> and who is acting as a Processor of Personal data: Customer, reg.no. <number>.

Personal data means any information directly or indirectly related to the Client and which is classified as 'personal data' according to EU General Data Protection Regulation 2016/679.

Processing means any operation carried out with Personal data (incl. collection, recording, storing, alteration, grant of access to, making enquiries, transfer, etc.) according to EU General Data Protection Regulation 2016/679.

The Company means any legal entity whose registered office is in Lithuania and who is acting as a Processor of Personal data: UAB Softera Baltic, reg.no. 301566552 in K. Donelaičio str. 62/V. Putvinskio str. 53 LT-44248, Kaunas Lithuania or entities that are performing Processing tasks on behalf of the company.

2. General provisions

2.1 These principles describe how the Company Processes Personal data on a general level. Specific details on the Processing of Personal data might be also described in agreements, other service related documents.

2.2 The Company ensures, within the framework of applicable law, the confidentiality of Personal data and has implemented appropriate technical and organisational measures to safeguard Personal data from unauthorized access, unlawful Processing or disclosure, accidental loss, modification or destruction.

2.3 The company may use authorised processors for Processing Personal data. In such cases, the Company takes needed steps to ensure that such data processors Process Personal data under the instructions of the Company and in compliance with applicable law and requires adequate security measures.

3. Categories of Personal data

Personal data may be received from the Client for processing, collected from the Client, from the Client's use of the services and from external sources such as public and private registers or other third parties. Personal data categories which THE COMPANY primarily, but not only, collects and processes are:

- **Identification data** such as name, personal identification code, date of birth, data regarding the identification document (such as copy of the passport, ID card, Contact data such as address, telephone number, email address.
- **Professional data** such as educational or professional career.
- **Financial data** such as accounts, ownership, transactions, credits, income, liabilities, the Client's financial experience and cooperation objectives such as data collected during the selection and provision of a variety of engineering services.

- **Data about trustworthiness and due diligence** such as data about payment behavior, damage caused to THE COMPANY or any third party.
- **Data obtained and/or created while performing an obligation arising from law** such as data resulting from enquiries made by investigative bodies, notaries, tax administrator, courts and bailiffs, details of income, credit commitments, property holdings, remarks, historical remarks and debt balances.
- **Data about the Client's tax residency** such as data about the country of residence, tax identification number, citizenship.
- **Data related to the services such as the performance of the agreements or the failure** thereof, executed transactions, concluded and expired agreements, submitted applications, requests and complaints, interests and service fees, insurance experience.
- **Data about habits, preferences and satisfaction** such as the activeness of using the services, services used, Client satisfaction.
- Any Personal data directly or indirectly collected by the Client and handed over to the Company for Processing.

4. Purposes and basis of Processing Personal data

The Company processes Personal data primarily to:

4.1 Perform Processing operations requested by the Client

To perform the consulting, development, maintenance, analysis, monitoring and other tasks defined in contracts between the Client and the Company.

4.2 Protect interest of the Client and/or the Company

To protect the interests of the Client and/or the Company and examine the quality of services provided by the Company and for the purpose of providing proof of a commercial transaction or of other business communication based on: performance of an agreement or in order to take steps at the request of the Client prior to entering into an agreement or compliance with a legal obligation or consent from the Client or the Company legitimate interests to prevent, limit and investigate any misuse or unlawful use or disturbance of the Company services and products, internal training or quality assurance of services. To guarantee the security the Company and/or the Client and other rights of the Company and the Client based on: the Company legitimate interest to protect its Clients, employees, visitors and theirs and the Company assets.

4.3 Comply with legal obligations

To comply with applicable law and international agreements, or compliance with a legal obligation.

4.4 Establishing, exercising and defending legal claims

To establish, exercise, assign and defend legal claims based on: performance of an agreement or in order to take steps at the request of the Client prior to entering into an agreement or compliance with a legal obligation or the Company legitimate interests to exercising legal claims.

5. Recipients of Personal data

Personal data is shared with other recipients, such as:

5.1 Authorities (such as law enforcement authorities, bailiffs, notary offices, tax authorities, supervision authorities).

5.2 Auditors, legal and financial consultants, or any other processor authorized by the Company.

5.3 Other persons related to provision of services of the Company such as providers of archiving, postal services, providers of services rendered to the Client.

6. Geographical area of Processing

6.1 As a general rule the Personal data is processed within the European Union/European Economic Area (EU/EEA) but in some cases transferred and processed to countries outside the EU/EEA.

6.2 Transfer and Processing of Personal data outside the EU/EEA can take place provided there is a legal ground, i.e. legal requirement conclusion or performance of an agreement or Client's consent and appropriate safeguards are in place. Appropriate safeguards, such as:

- There is an agreement in place including the EU Standard Contractual Clauses or other approved clauses code of conducts, certifications etc., approved in accordance with the General Data Protection Regulation;
- The country outside of the EU/EEA where the recipient is located has adequate level of data protection as decided by the EU Commission;
- The recipient is certified under the Privacy shield (applies to recipients located in the United States).

6.3 Upon request the Client can receive further details on Personal data transfers to countries outside the EU/EEA.

7. Retention periods

Personal data will be processed no longer than necessary. The retention period may be based on agreements with the Client, the legitimate interest of the Company or applicable law (such as laws related to bookkeeping, statute of limitations, civil law, etc.).

8. Obligation of UAB Softera Baltic

In view of the foregoing, the UAB Softera Baltic undertakes, for all data processed in its internal development environment and any interface with it, to:

- Treat the data only for the single purpose (s) that are / are the subject of the subcontracting,
- Process the data in accordance with the documented instructions of The Client. If UAB Softera Baltic considers that an instruction constitutes a violation of the European Data Protection Regulation or any other provision of Union law or the law of the Member States relating to data protection, it shall immediately inform the Client thereof any means written at his convenience. In addition, if UAB Softera Baltic is required to transfer data to a third country or to an international organization, under Union law or the law of the Member State to which it is subject, it must inform the Client processing this legal obligation prior to processing, unless the right concerned prohibits such information for important reasons of public interest
- Guarantee the confidentiality of the personal data processed under the Contract,
- Ensure that persons authorized to process personal data under the Agreement:
 - o undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality
 - o receive the necessary training in the protection of personal data
- Take into account, with regard to its tools, products, applications or services, used and / or realized as part of the Services, the principles of data protection from conception and protection of data by default

UAB Softera Baltic shall notify The Client of any personal data breach within a maximum of twenty-four (24) hours after having read it by sending an e-mail addressed to the following address <email>, coupled with the sending within the same period of a registered letter with acknowledgment of receipt. This notification shall be accompanied by all relevant documentation in order to enable the controller, if necessary, to notify that breach to the competent supervisory authority.

UAB Softera Baltic undertakes to implement the following security measures, on all personal data stored in its environments:

- pseudonymisation and encryption of personal data
- Ways to ensure the ongoing confidentiality, integrity, availability and resilience of treatment systems and services;
- the means to restore the availability of personal data and access to it in good time in the event of a physical or technical incident;
- a procedure to test, analyze and regularly evaluate the effectiveness of technical and organizational measures to ensure the safety of treatment

UAB Softera Baltic represents and warrants to keep in writing a register of all categories of processing activities performed on behalf of the Customer including:

- the name and contact details of the controller on whose behalf he acts, any subcontractors and, where applicable, the data protection officer;
- categories of treatments performed on behalf of The Client;
- where appropriate, the transfer of personal data to a third country or to an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in Article 49, second subparagraph of the European Data Protection Regulation, documents proving the existence of appropriate safeguards.

Finally, at the The Client's first request and, in any event, at the end of each calendar month, the UAB Softera Baltic undertakes to destroy and not retain any personal data transmitted by the The Client.

9. Contact details

8.1 Clients may contact the Company with any enquiries, withdrawal of consents, requests to exercise data subject rights and complaints regarding the use of Personal data.

8.2 Contact details of the company are available on the Company website: www.softera.lt

8.3 Contact details of the appointed responsible person: gabriele.stasiunaite@softera.lt, marked "Data Protection".

10. Validity and amendments of the principles

10.1 The Company is entitled to unilaterally amend the principles at any time, in compliance with the applicable law, by notifying the Client of any amendments via website of the Company, or via post, via e-mails or another manner (for example through mass media), not later than one month prior to the amendments entering into force.