DATA PROCESSING CODE

1. Purpose of this document

The purpose of this document is

a) regulate in a single framework the requirements for the data Processors employed by the Controller; and to

b) assist compliance with the requirements of the legal regulations on data protection and the implementation of adequate technical and organisational measures for the protection of the right of the data subjects.

2. Interpretative Provisions

„GDPR":

Regulation of the European Parliament and of the Council (EU) 2016/679 (27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation 95/46/EC

"Legal regulations on data protection":

Legal regulations relating to the control, processing, protection and use of personal data, the Controller and the Processor employed by them as well as the services provided by the Processor.

Including especially, but not limited to, the following:

a) GDPR,

b) Act CXII of 2011 on Informational Self-determination and Freedom of Information (hereinafter Hungarian abbreviation: Infotv.).

c) Act C of 2003 on Electronic Communications;

d) any court or authority interpretation of the above or any guidance, guide or practical regulation issued by any competent supervisory authority, an approved code of conduct or an approved certification mechanism.

The legal regulations listed in sub-paragraphs a)-c) refer to their currently effective versions.

"Personal data":

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Processing":

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“Controller”:

For the purposes of this document Invitech ICT Services Ltd. or any company controlled by, controlling or under common control with Invitech ICT Services Ltd. is considered the Controller with which the Processor has a contract.

“Processor”:

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller. For the purposes of this document the Processor is a contracted partner of the Controller who or which takes part in the processing of personal data.

“Sub-Processor”:

Further data processor employed by the Processor for the processing activity.

“Personal data breach”:

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

“Contract”:

The agreement between the Controller and the Processor, based on which the Processor processes Personal Data on the order of the Controller.

“Code”:

This document.

The terms and definitions not defined in this Code shall be interpreted with the same meaning as specified in the legal regulations on Data Protection.

3. Interpretation and applicability:

3.1. This Code applies to the processing of personal data.

3.2. The provisions of this Code shall be applied from 25 May 2018.

3.3. The currently effective provisions of this Code constitute an annex to the respective and effective contract between the Processor and the Controller for the processing of Personal Data.

3.4. The effective text of the Code is accessible on the Controller’s website and constitutes part of the contract without any specific notification.

4. Instructions for data processing

4.1. When the Processor processes Personal Data on the Controller’s order, the Processor:

a) processes the personal data only on written (documented) instructions from the Controller, including with regard to transfers of personal data to a third country or an international organisation;

b) processes the personal data only on instructions on processing unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

c) and notifies the Controller in writing without any delay when, according to their opinion, any instruction is contrary to the legal regulations on Data Protection and justifies that opinion.

4.2. Primarily the tasks specified in the contract shall be deemed as written Controller instructions. With regard to any case not regulated in the contract, the written instructions shall be governed by the provisions of the contract pertaining to contact. Without those any posted mail, fax message or electronic mail sent by one Party to another shall be deemed a written instruction.

4.3. The Controller and Processor shall take steps to ensure that any natural person acting under the authority of the Controller or the Processor who has access to personal data does not process them except on instructions from the Controller, unless he or she is required to do so by Union or Member State law.

4.4. When the Processor does not proceed in accordance with the Controller's instructions, the Controller shall have the right to terminate the contract. In that case the Processor shall bear the consequences of termination of the contract as specified therein, also including any penalty or compensation claims of the Controller.

5. Confidentiality

5.1. The Processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. When the Controller requests, the Processor shall make available for the Controller immediately the documents supporting the agreement to confidentiality.

5.2. The Processor shall take all reasonable steps to ensure the reliability of the authorised individuals processing Personal Data and that the authorised individuals processing Personal Data receive adequate training on compliance with the legal regulations on Data Protection pertaining to processing.

6. Security of processing

6.1. The Processor introduces and maintains adequate technical and organisational measures in relation to the processing of Personal Data in compliance with the contract at their own cost.

6.2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

7. Use of other processors (sub-processors)

7.1. The Processor shall not engage another processor without prior specific or general written authorisation of the Controller.

7.2. In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors (sub-processors), thereby giving the Controller the opportunity to object to such changes.

7.3. When the Controller has consented to the involvement of another Processor, the Processor appoints the sub-processor in a written agreement. The agreement on the employment of a sub-processor shall include the same Data Protection obligations as the obligations prevailing between the Processor and the Controller.

In particular:

a) the sub-Processor shall provide adequate guarantees for implementing adequate technical and organisational measures to make sure that Data Processing complies with the provisions of the legal regulations on Data Protection and

b) shall also comply with the requirements of this Code.

7.4. The Processor shall inform the Controller of the involvement of a sub-Processor and the relevant terms and conditions of the processing contract simultaneously with the establishment of the agreement.

7.5. Where that sub-Processor fails to fulfil its data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of that sub-Processor's obligations.

8. Technical and organisational measures

8.1. Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights.

8.2. The Processor keeps records without any fee and provides all information to the Controller immediately, or not later than within 5 days from its receipt

a) on all requests received from data subject and

b) on all Data Protection complaints relating to the processing of Personal Data.

8.3. The Processor cooperates with the Controller in the investigations of the request or complaints of the data subjects. The Processor may send a response to the data subjects only with the prior written approval of the Controller.

9. Deletion and return of personal data

9.1. The Processor shall proceed in compliance with the provisions of the contract for the deletion of Personal Data and for returning them to the Controller when the processing activity ceases for any reason.

9.2. Without any contractual provision the Processor shall securely delete all Personal Data upon the Controller’s written instruction without any delay or shall securely return them to the Processor after the completion of the processing activity.

9.3. The obligation specified in the previous paragraphs does not apply when the EU or Member State legislation requires the storage of Personal Data.

10. Records of processing activities

10.1. The Processor shall maintain a record of all categories of processing activities carried out on behalf of a Controller.

10.2. That record shall contain the following information:

a) the name and contact details of the Processor or Processors and of each Controller on behalf of which the Processor is acting, and, where applicable, of the Controller 's or the Processor's representative, and the data protection officer;

b) the categories of processing carried out on behalf of the Controller ;

c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation;

d) and the documentation of the technical and organisational measures.

10.3. The data processing records shall be kept in writing, including in electronic form.

10.4. The Controller or the Processor and, where applicable, the Controller's or the Processor's representative, shall make the record available to the supervisory authority on request.

10.5. The record keeping obligations referred to in this paragraph 10 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

11. Providing information, cooperation and control

11.1. The Processor shall make available to the Controller all information which certifies that the Processor fulfilled all the obligations prevailing according to the legal regulations on Data Protections and this Code also including information relating to the technical and organisational measures introduced and maintained by the Processor.

11.2. The Processor should assist the Controller in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

11.3. The Processor allows for and contributes to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

11.4. If during any audit or on the spot check it turns out that the Processor failed to substantially comply with the obligations specified in the legal regulations on Data Protection or violated them, the Processor shall reimburse the equitable costs of the Processor or the auditors authorised by them, or of the audit or on the spot checks.

11.5. The Processor shall eliminate any inadequacy and problem relating to Data Protection and Data Security, identified by the Controller and indicated to the Processor without any delay, at their own cost when they suggest that the Processor or any sub-Processor did not fulfil the obligations under this contract or under this Code.

11.6. If the Processor fails to fulfil the obligations prevailing under the contract or under this Code, the Controller may suspend the transfer of Personal Data to the Processor until the default is remedied.

11.7. The Processor informs the Controller when they join a code of conduct or a certification mechanism. That information may be used as part of proof that the Processor ensures the data processing guarantees required under the legal regulations on Data Protection.

11.8. The Processor shall ensure that the sub-Processors also comply with the provisions of this paragraph.

12. Rules applicable in the case of personal data breach

12.1. The Processor shall notify the Controller without undue delay, or no later than within 12 hours from becoming aware of a personal data breach.

12.2. The Processor shall, within the shortest possible time, or not later than within 24 hours from becoming aware of them, send information to the Controller and

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

12.3. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

12.4. The Processor shall cooperate with the Controller to the extent required and assist the Controller in any corrective measure relating to Personal Data Breach, also including information sent to data subjects.

13. Liability and compensation

13.1. The Processor shall be fully liable for compensation for any damage that is the consequences of processing pursued by them, including especially when

a) the Processor or any sub-processor failed to fulfil any obligation under this Code or the legal regulations on data protection, or

b) the Processor or any sub-processor did not proceed in accordance with the Controller's lawful instructions on Personal Data processing.

Budapest, 01 Apr 2023