

# CerTrust Inspection and Certification Ltd.

## General Data Protection Regulation (GDPR)

A handwritten signature in blue ink, appearing to read "Tasnádi", is positioned above a horizontal dotted line.

**Gábor Tasnádi**

Managing Director

(came into force on 20.05.2019)

**Tartalomjegyzék**

1. The purpose of the Regulations .....	3
2. Scope .....	3
3. Definitions .....	3
4. Principles for handling personal data.....	3
4.1 Pursuant to Article 5 of the GDPR regulation.....	3
5. The legal basis and purpose of individual data management.....	4
5.1 Lawfulness of data management: .....	4
5.2 Data management for purposes other than the purpose of data collection.....	5
5.3 Terms of consent.....	5
5.4 Management of the data of employees and persons holding positions in the company (hereinafter referred to as internal persons).....	5
5.5 Management of the data of employees, representatives and other natural persons (hereinafter referred to as external persons) of legal or unincorporated organizations or persons related to CerTrust.....	6
5.6 Management of special categories of personal data .....	6
6. Method of data management .....	6
7. Duration of data management.....	6
8. Disposal of personal data .....	6
8.1. Information to be made available .....	6
8.2 The data subject's right of access.....	8
8.3 The data subject's right to correction, deletion and restriction of data processing.....	8
8.4 Right to data portability .....	9
8.5 Right to protest.....	9
9. Data processing .....	9
10. Registration of data management activities .....	9
11. Data protection incidents.....	10
12. Data protection impact assessment.....	11
13. Modification of the Data Management Policy .....	11
14. Enforcement options.....	12

## **1. The purpose of the Regulations**

The purpose of regulation is to record the practices used by CerTrust Inspection and Certification Ltd (1134 Budapest, Váci road 49. (DC offices). 6. floor, 01 09 384979, hereinafter: CerTrust) in the course of its general activity and operation, as well as in the provision of services related to the information society - general and with particular regard to the data protection and management principles for the personal data of natural persons and CerTrust's data protection and management policy, which CerTrust recognizes as binding on itself.

When creating these rules, CerTrust took particular account of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free flow of such data, as well as on the repeal of Regulation 95/46/EC (general data protection regulation - hereinafter "GDPR regulation"), and CXII of 2011. the prescribed provisions of the Act on the right to informational self-determination and freedom of information ("Infotv.").

## **2. Scope**

The scope of these regulations covers the following data management:

- data management related to employees and persons holding positions in the company;
- data management of external natural persons who are directly or indirectly connected and affected during or in connection with CerTrust's activities - regardless of the legal relationship CerTrust has with the following legal or unincorporated organizations or individuals with the data subject:
  - economic companies,
  - other organizations,
  - individual entrepreneurs,
  - natural persons;
- other - according to Article 4 of the GDPR regulation - data management.

## **3. Definitions**

Article 4 of the GDPR regulation and Infotv. definitions are applied.

## **4. Principles for handling personal data**

### **4.1 Pursuant to Article 5 of the GDPR regulation**

1. CerTrust regarding personal data:
  - a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
  - b) 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');
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
  - d) 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');
  - e) 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');
  - f) 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').
  - g) **accountability** – CerTrust is responsible for, and be able to demonstrate compliance with, paragraph 1
2. The above principles regarding the handling of personal data and their interpretation are supplemented by Info tv. in accordance with § 4.
3. Additional provisions of data management principles:
- a) During data processing, personal data will retain its quality as long as the relationship with the data subject can be restored. The relationship with the data subject can be restored if the data controller has the technical conditions necessary for the restoration;
  - b) CerTrust undertakes to handle the data in its possession in accordance with the legal regulations and the data protection principles set out in these Regulations.

## **5. The legal basis and purpose of individual data management**

### **5.1 Lawfulness of data management:**

CerTrust only handles personal data if and only if at least one of the following is fulfilled and can be considered verified:

- a) the data subject has given her consent to the processing of her personal data for one or more specific purposes;
- b) data management is necessary for the performance of a contract in which the data subject is one of the parties, or it is necessary for taking steps at the request of the data subject prior to the conclusion of the contract;
- c) data management is necessary to fulfill a legal obligation concerning CerTrust as a data controller (in this case, EU or relevant national law may determine the legal basis, in which case the purpose of data management must be determined with reference to this legal basis);
- d) data processing is necessary to protect the vital interests of the data subject or another natural person;
- e) data management is in the public interest or is necessary for the execution of a task performed in the context of the exercise of the public authority delegated to CerTrust as the data controller;

- f) data management is necessary to enforce the legitimate interests of CerTrust as a data controller or a third party, unless the interests or fundamental rights and freedoms of the data subject that require the protection of personal data take priority over these interests, especially if the data subject is a child.

## **5.2 Data management for purposes other than the purpose of data collection**

In all cases, if CerTrust intends to use the provided data for a purpose other than the purpose of the original data collection, it informs the data subject and obtains their prior, express consent, or provides them with the opportunity to prohibit the use.

CerTrust can only use a procedure different from the above in the case according to Article 23 of the GDPR regulation - including the restrictions if data processing for a purpose other than the purpose of data collection is not based on the consent of the data subject or any EU or member state law.

## **5.3 Terms of consent**

If the data management is based on consent, CerTrust, as a data manager, ensures and certifiably documents that the data subject has consented to the management of his personal data. The consent of the data subject can be given (not exclusively) in the context of the written statement recorded in the given annex.

The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the legality of data processing based on consent prior to withdrawal. The consent can be revoked by the person concerned in writing, clearly referring to the relevant statement.

When giving consent, CerTrust treats the principle of data economy and purposefulness as a priority requirement, and does not initiate a request for consent to the processing of personal data that is not necessary for data management or the fulfillment of the relevant contract - including the provision of services.

## **5.4 Management of the data of employees and persons holding positions in the company (hereinafter referred to as internal persons).**

The data of CerTrust's internal persons is managed in order to fulfill the employer's obligations contained in Act I of 2012, as well as to fulfill the reporting, registration, reporting and other obligations prescribed in connection with the employment relationship. Consent to data management is voluntary and is considered to be given by signing the employment contract. Data may be transferred to CerTrust, which also processes data for payroll and other employment purposes for CerTrust. As an accounting service provider, consent to data transfer is considered to be given by signing the employment contract.

CerTrust processes the personal data contained in the CVs and other attached documents received directly or through an employment intermediary for the purpose of informing the person concerned about the vacant position at CerTrust, the conditions for applying for it, arranging an appointment with the person concerned, and carrying out the selection. Data management is based on the voluntary consent of the person concerned, which consent is given by the person concerned by sending his/her CV and related documents (e.g. documents proving qualifications, education, criminal record).

Data will be transferred in order to exercise rights and fulfill obligations related to the employment relationship in cases that cannot be individually determined in advance (e.g. to a lawyer providing legal

representation in the case of an employment dispute), consent to data transfer is considered to be given by signing the employment contract.

### **5.5 Management of the data of employees, representatives and other natural persons (hereinafter referred to as external persons) of legal or unincorporated organizations or persons related to CerTrust**

The data of external persons connected to CerTrust is processed in order to enforce and fulfill the rights and obligations assumed in the business relationship between CerTrust and the relevant party. The consent is voluntary, and in view of the fact that the person concerned has been named for the benefit of a person independent of CerTrust, the consent is deemed to be given by signing a contract, declaration, other agreement signed between this independent party and CerTrust, or by establishing a legal relationship with the named in a circle named in documents and legal relationships.

### **5.6 Management of special categories of personal data**

When handling possible special categories of personal data, CerTrust acts in accordance with Article 9 of the GDPR regulation, taking it into account and complying with it.

## **6. Method of data management**

The data is handled by electronic means, not in an automated way, and on a paper basis. During the electronic data management, the servers and devices for storage are located in Hungary, while the paper-based data management takes place in the official premises of CerTrust.

## **7. Duration of data management**

The data storage period for each data management purpose is as follows:

- 1) The duration of data management according to points 5.4 and 5.5 lasts until the achievement of the relevant data management goal or its failure, taking into account the existence of the legal relationship serving as the legal basis for data management. An exception is the period after the termination of the relevant legal basis, during which CerTrust is obliged to record the relevant data;
- 2) Beyond the period included in point 1) in the event that there is a case related to the data subject in progress, during which the processing of personal data is necessary - including, in particular, data processing related to the fulfillment of the legal obligation of the data controller;
- 3) The Data Controller reserves the right to store for an unlimited period of time for statistical and analytical purposes data whose connection with the data subject cannot be restored after the expiration of the time available for storing personal data.

## **8. Disposal of personal data**

### **8.1. Information to be made available**

- 1) If CerTrust collects the personal data concerning the data subject from the data subject, CerTrust, as a data controller, provides all of the following information to the data subject at the time of obtaining the personal data:
  - the contact details of CerTrust as a data controller;
  - contact details of the data protection officer;
  - the purpose of the planned processing of personal data;

- the legal basis for data management
- in the case of data management based on point f) of Article 6 (1) of the GDPR regulation, the legitimate interests of the data controller or a third party;
- where appropriate, recipients of personal data and categories of recipients, if any;
- where applicable, the fact that CerTrust, as a data controller, wishes to transfer personal data to a third country or an international company, as well as the existence or absence of a Commission compliance decision, or in Article 46, Article 47 or Article 49 ( In the case of data transfer referred to in the second subparagraph of paragraph 1), the indication of suitable and suitable guarantees, as well as a reference to the methods for obtaining a copy of them or their availability.

In order to ensure fair and transparent data management, CerTrust informs the data subject of the following additional information:

- the duration of storage of personal data, or if this is not possible, the criteria for determining this duration;
  - the data subject's right to request from the data controller access to personal data relating to her, their correction, deletion or restriction of processing, and to object to the processing of such personal data, as well as the data subject's right to data portability;
  - in the case of data processing based on point a) of Article 6 (1) or point a) of Article 9 (2) of the GDPR regulation, the right to withdraw consent at any time, which does not affect the legality of data processing carried out on the basis of consent before the withdrawal ; d) on the right to submit a complaint to the supervisory authority; e) whether the provision of personal data is based on legislation or contractual obligations or is a prerequisite for concluding a contract, and whether the data subject is obliged to provide personal data.
- 2) If CerTrust does not collect personal data about the data subject from the data subject, CerTrust, as a data controller, provides the data subject with the following information:
- the contact details of CerTrust as a data controller;
  - contact details of the data protection officer;
  - the purpose of the planned processing of personal data;
  - the legal basis for data management;
  - categories of personal data concerned;
  - where appropriate, recipients of personal data and categories of recipients, if any;
  - where applicable, the fact that CerTrust, as a data controller, wishes to transfer personal data to a third country or an international company, as well as the existence or absence of a Commission compliance decision, or in Article 46, Article 47 or Article 49 ( In the case of data transfer referred to in the second subparagraph of paragraph 1), the indication of suitable and suitable guarantees, as well as a reference to the methods for obtaining a copy of them or their availability.

In order to ensure fair and transparent data management, CerTrust informs the data subject of the following additional information:

- the duration of storage of personal data, or if this is not possible, the criteria for determining this duration;

- in the case of data management based on point f) of Article 6 (1) of the GDPR regulation, the legitimate interests of the data controller or a third party;
- the data subject's right to request from the data controller access to personal data relating to her, their correction, deletion or restriction of processing, and to object to the processing of such personal data, as well as the data subject's right to data portability;
- in the case of data processing based on point a) of Article 6 (1) or point a) of Article 9 (2) of the GDPR regulation, the right to withdraw consent at any time, which does not affect the legality of data processing carried out on the basis of consent before the withdrawal ; d) on the right to submit a complaint to the supervisory authority; e) on whether the provision of personal data is based on legislation or a contractual obligation or is a prerequisite for the conclusion of a contract, and whether the data subject is obliged to provide personal data;
- the right to submit a complaint addressed to a supervisory authority;
- the source of the personal data and, where applicable, whether the data comes from publicly available sources.

The provisions in points 1) and 2) do not apply if:

- the data subject already has the relevant information;
- providing the information in question proves to be impossible or would require a disproportionately large effort.

### **8.2 The data subject's right of access**

The data subject has the right to request and receive feedback from CerTrust on whether his personal data is being processed, and if such data processing is in progress, he is entitled to request that personal data and (detailed under Article 15 of the GDPR regulation) receive access to information based on your written request within 30 days.

### **8.3 The data subject's right to correction, deletion and restriction of data processing**

- 1) The data subject has the right to submit a written request for the correction of inaccurate personal data concerning him/her, to which CerTrust is obliged to correct the relevant data within 30 days. Taking into account the purpose of the data management, the data subject is entitled to request the completion of incomplete personal data, including by means of a supplementary statement.
- 2) The data subject has the right to request the deletion of his personal data from CerTrust. CerTrust, as a data controller, deletes the personal data of the data subject without undue delay if one of the following reasons applies:
  - the personal data are no longer needed for the purpose for which CerTrust collected or otherwise processed them;
  - the data subject withdraws his/her consent, which is the basis of the data processing pursuant to point a) of Article 6 (1) or point a) of Article 9 (2), and there is no other legal basis for the data processing;
  - the data subject objects to the data processing based on Article 21 (1), and there is no overriding legal reason for the data processing, or the data subject objects to the data processing based on Article 21 (2);
  - if the personal data was handled illegally by CerTrust;



- personal data must be deleted in order to fulfill CerTrust's legal obligations under EU or Member State law applicable to the data controller.
- 3) The data subject has the right to have the data controller restrict data processing with regard to the personal data related to him/her, based on his/her written request, if one of the conditions of Article 18 of the GDPR regulation is met.
  - 4) CerTrust informs all recipients of all corrections, deletions or data management restrictions according to points a), b) and c) to whom or to whom the personal data has been communicated, unless this proves to be impossible or requires a disproportionately large effort. Upon separate written request, CerTrust informs the data subject about these recipients.
  - 5) Written order

The data subject can request information about the processing of their personal data from CerTrust at any time in writing, by registered letter or by registered mail sent to CerTrust's address. CerTrust fulfills the request for information sent by letter if the person concerned can be clearly identified based on the sent request. CerTrust considers a request for information sent by e-mail as authentic only if it is sent from the e-mail address recorded in advance in writing. The request for information may cover the data subject's data managed by CerTrust, their source, the purpose, legal basis, duration of data processing, the name and address of any data processor, the activities related to data processing, and, in the case of transmission of personal data, who received it and for what purpose and the data of the data subject, unless the provision of information is prohibited by law in relation to data transmission.

The Data Controller must respond to questions related to data management within 30 days of receipt. In the case of e-mail, the date of receipt shall be considered the first working day after sending.

### **8.4 Right to data portability**

Based on her written request, the data subject is entitled to receive her personal data provided to CerTrust in a segmented, widely used, machine-readable format.

### **8.5 Right to protest**

The data subject - in a written action - has the right to object at any time for reasons related to his own situation against the processing of his personal data based on points e) or f) of Article 6 (1) of the GDPR regulation, including profiling based on the aforementioned provisions. In this case, CerTrust will no longer process the personal data, unless it is proven that the data processing is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or that are necessary for the presentation, enforcement or defense of legal claims. are connected.

## **9. Data processing**

CerTrust is entitled to use a data processor, the circumstances, conditions and application of which can be exercised based on the provisions of Article 28 of the GDPR regulation.

Data processing is typically related to the following activities: payroll, accounting, fulfillment of agreements related to the implementation of economic activity.

## **10. Registration of data management activities**

CerTrust keeps a record of its data management activities, with regard to Article 30 (5) of the GDPR regulation.

- 1) CerTrust, as a data controller, keeps records of its data management activities. This register contains the following information:
  - name and contact information of data controller,
  - the name and contact information of the data controller's representative;
  - the name and contact information of the data protection officer / agent;
  - the purposes of data management;
  - description of categories of data subjects and categories of personal data;
  - categories of recipients to whom the personal data is or will be communicated, including recipients in third countries or international companies;
  - where appropriate, information on the transfer of personal data to a third country or international company, including the identification of the third country or international company, and in the case of transfer according to the second subparagraph of Article 49 (1), a description of the appropriate guarantees;
    - if possible, deadlines for deleting different data categories;
    - if possible, a general description of the technical and organizational measures mentioned in Article 32 (1) of the GDPR regulation.
- 2) As a data processor, CerTrust keeps records of all categories of data management activities performed on behalf of the relevant data controller. This register contains the following information:
  - the name and contact details of the data processor or data processors,
  - the name and contact details of all data controllers on whose behalf the data processor acts;
  - the name and contact information of the representative of the data manager or data processor;
  - the name and contact information of the data protection officer / representative;
  - categories of data management activities performed on behalf of individual data controllers;
  - where appropriate, information on the transfer of personal data to a third country or international company, including the identification of the third country or international company, and in the case of transfer according to the second subparagraph of Article 49 (1), a description of the appropriate guarantees;
  - if possible, a general description of the technical and organizational measures referred to in Article 32 (1) of the GDPR regulation.

CerTrust keeps the records recorded in points 1) and 2) in writing (in electronic format). CerTrust ensures that, upon request, it will provide the above-referenced records to the supervisory authority.

### **11. Data protection incidents**

In the event of a possible data protection incident, CerTrust acts as follows:

- 1) CerTrust, as a data controller, shall report the data protection incident to the competent supervisory authority based on Article 55 of the GDPR without undue delay and, if possible, no later than 72 hours after the data protection incident became known, unless the data protection incident is likely there is no risk to the rights and freedoms of natural persons. The notification shall contain at least the following:

- the nature of the data protection incident, including – if possible – the categories and approximate number of affected persons, as well as the categories and approximate number of data affected by the incident;
- the name and contact details of the data protection officer / agent or other contact person providing additional information;
- probable consequences resulting from the data protection incident;
- the measures taken or planned by the data controller to remedy the data protection incident, including, where appropriate, measures aimed at mitigating any adverse consequences resulting from the data protection incident.

If and to the extent that it is not possible to provide the information simultaneously, it will be provided in parts.

- 2) If the notification is not made within 72 hours, CerTrust will attach the reasons to justify the delay to the notification.
- 3) CerTrust ensures – if it is involved as a data processor in the detected data protection incident – that it reports it to the relevant data controller without undue delay after becoming aware of it.
- 4) If the data protection incident is likely to involve a high risk for the rights and freedoms of natural persons, CerTrust, as a data controller, shall inform the data subject(s) of the data protection incident without undue delay.
- 5) CerTrust does not provide information to the data subject(s) if any of the following conditions are met:
  - CerTrust has implemented appropriate technical and organizational protection measures and these measures have been applied to the data affected by the data breach, in particular those measures - such as the use of encryption - that make the personal data unintelligible to persons not authorized to access it the data;
  - after the data protection incident, CerTrust took additional measures to ensure that the high risk to the rights and freedoms of the data subject(s) referred to in point d) is unlikely to materialize in the future;
  - providing information would require a disproportionate effort. In such cases, CerTrust informs the data subjects via publicly published information, or takes a similar measure that ensures similarly effective information to the data subjects.

CerTrust keeps a register for the purpose of monitoring the measures related to the data protection incident and for informing the affected parties, which contains the facts related to the data protection incident, its effects and the measures taken to remedy it.

### **12. Data protection impact assessment**

CerTrust - if any type of data management (taking into account its nature, scope, circumstances and purposes) is likely to involve a high risk for the rights and freedoms of natural persons - prior to data management, CerTrust performs an impact assessment on how the planned data management operations affect the protection of personal data . During each data protection impact assessment, CerTrust takes Article 35 of the GDPR regulation into account and acts accordingly.

### **13. Modification of the Data Management Policy**

CerTrust may unilaterally change this Privacy and Data Management Policy (GDPR) at any time.

### 14. Enforcement options

The rights enforcement options of the data subject are set out in the GDPR regulation, Infotv. and pursuant to Act V of 2013 (Ptk.), you can also request the help of the National Data Protection and Freedom of Information Authority (1125 Budapest Szilágyi Erzsébet fasor 22/C; postal address: 1530 Budapest, Pf. 5).