Privacy policy

Content

Introduction

TC&C Ltd. (headquarters: 1134 35. Wesselényi str. Budapest, Hungary company registration number: 01-09-168656) (hereinafter referred to as "**Data Controller**" or "**TC&C**") created this data control regulation.

This document is based on paragraph 77 of the preamble to the European Parliament and Council Regulation (EU) 2016/679 (hereinafter referred to as the "GDPR"), Act CXII of 2011 on Informational Self-determination and Freedom of Information (hereinafter referred to as the "Info tv"), and other relevant legal regulations contains the data control information of TC&C Ltd..

Whenever this Regulation relates to "article", should be considered to be an article of GDPR.

1. Basic Principles

Lawfulness, fairness, transparency

The control of personal data can only be done on the basis of a specific legal basis (an agreement or other legitimate legal basis). Personal data should be controlled fairly and transparently. Information about data control needs to be provided in an accurate, transparent, comprehensible and easily accessible form with simple and comprehensible language.

Purpose limitation

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.

Data minimisation

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

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.

Storage limitation

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 GDPR in order to safeguard the rights and freedoms of the data subject.

Integrity and confidentiality

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. It primarily takes precautionary measures on IT and organizational aspects (eg access and eligibility procedures, coding), taking into account, in particular, the provisions of Article 32 (Privacy of Data Management) and Article 35 (Data Protection Impact Assessment) of GDPR. Data protection incidents, ie personal data breaches, if there is a risk of infringing the data subjects' rights, the data protection authority must be notified pursuant to Article 33 of the GDPR. If applicable, if the risk is high, data subject must be notified directly.

Accountability

The controller shall be responsible for, and be able to demonstrate compliance with documents, agreements, written consents, legal basis etc…

I. Data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-

readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

II. Transparent information, communication and modalities for the exercise of the rights of the data subject

Before any data processing is initiated, the data subject must be clearly and thoroughly informed of all the facts related to his or her data, in particular:

- **purpose and legal basis,**
- **the person authorized for data processing and processing,**
- **the duration of the data processing,**

Data subject shall be informed about every legal basis of data processing especially but not solely if
• It is necessary to comply with a legal obligation for the data controller, or
• it is necessary to enforce the legitimate interest of the data controller or third party and the enforcement of this interest is proportionate to limiting the right to the protection of personal data.

The information shall also include the rights and remedies available to the data subject.

If the personal information of the data subjects would be impossible or disproportionate (such as a website) information may also be disclosed by disclosing the following information:
(a) the fact of collecting data,
b) information of data subjects,
(c) the purpose of the collection of data,
(d) the duration of the processing,
e) the person who is able to access the data,
(f) a description of the data management rights and remedies of the data subjects concerned

This Privacy Policy also governs the data management of the following website: http://www.tcandc.com/

2. Definitions

All the deffinitions are according to GDPR article 4.

For the purposes of this Regulation:

(1) **'personal data'** means 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;

(2) **'processing'** means 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;

(3) **'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;

(4) **'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) **'pseudonymisation'** means 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) **'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) **'third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) **'consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) **'personal data breach'** means 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;

(13) **'genetic data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) **'biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) **'data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) **'main establishment'** means:

(a) 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;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) **'representative'** means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) **'enterprise'** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) **'group of undertakings'** means a controlling undertaking and its controlled undertakings;

(20) **'binding corporate rules'** means personal data protection policies which are adhered to by a controller or processor established on the territory of a 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;

(21) **'supervisory authority'** means an independent public authority which is established by a Member State pursuant to Article 51;

(22) **'supervisory authority concerned'** means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) **'cross-border processing'** means either:

(a) 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 Union where the controller or processor is established in more than one Member State; or

(b) 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.

(24) **'relevant and reasoned objection'** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) **'information society service'** means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ([19]);

(26) **'international organisation'** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

3. Legal basis for data processing (Article 6 GDPR)

TC&C is both a data controller and data processor in relation of personal data process.

The processing of personal data shall be lawful only if it meets at least one of the following criteria:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

TC&C is processing personal data only on legal basis of article 6 1. (a), (b), (c), (f).

3. Purpose of data process

1. Personal data may only be processed for a specific purpose, for the exercise of the right and for the fulfillment of the obligation. At all stages of data management, the purpose of data management must be fulfilled, data acquisition and management must be fair and legitimate.

2. Only personal data that is essential for achieving the purpose of data management can be processed to achieve the specific purpose. Personal data can only be processed to the extent and for the duration required to achieve the purpose.

4. Other Principles

Personal data preserves this quality while being processed as long as its connection can be restored with the data subject. The connection can be restored if the data controller has the necessary technical conditions for restoration.
Data management shall ensure the accuracy and completeness of the data and, where necessary for the purposes of data management, the updating of the data and ensure, taht the identification of the data subject is possible as long as it is necessary for the porpuse of data processing.

(Info tv. 4.§ [3]-[4])

5. General rights of data subjects

TC&C shall provide the rights for data subject as described herunder:

Rights of data subjects

TC&C shall provide the information hereunder for data subjects.

a) Right for information

In particular, the data controller shall disclose the following information:

i. the relevant data of the subject
ii. the legal basis for their treatment
iii. the recipients of the data and the purpose of transormation
iv. the duration of the data handling or the criteria for determining it,
v. profiling
vi. the fact and circumstances of automated decision-making
vii. rights of data subjects

b) Right of Access

Pursuant to Article 15 of the GDPR, the data subject is entitled to receive feedback from the data controller as to whether his or her personal data is being processed and, if such processing is in progress, is entitled to access to personal data and relevant information.

c) Right to rectification

The data subject shall have the right to rectify any inaccurate personal data that he or she is entitled to request, without undue delay. Taking into account the purpose of data management, the person concerned has the right to request the addition of incomplete personal data, including by means of a supplementary statement.

d) Right to erasue (right to be forgotten)

In addition to the right to erasure, TC&C continuously provides for the possibility of withdrawing the consent for data process. If, in addition to the consent, the data management is implemented on the basis of another legal basis, erasure is not guaranteed.

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;

(c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). (children)

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. point 1. shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred to in point 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

e) Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing, pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under point 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the

establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

f) Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

g) Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent or on a contract, and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The right to data portability shall not adversely affect the rights and freedoms of others.

h) Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling based on those provisions. The controller shall no longer process the personal data unless:

- the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- processing is necessary for the legitimate interests of the data controller or a third party, except where the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, particularly where child is concerned

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

i) Right to appeal

From the right of appeal and the manner of enforcement, this information is provided in a separate chapter.

j) Complaints and requests for data handling

Position: HR Leader, or deputy
email: gdpr@tcandc.com

Remedies forum:

1. Metropolitan court of Budapest

2. Authority for Data Protection and Freedom of Information

   address: 22/C Szilágy Erzsébet fasor, Budapest 1125
   phone: +36 -1-391-1400
   email address: ugyfelszolgalat@naih.hu

6. General data control of CT&C (table)

TC&C may prosess personal data according to the table herunder:

scope of personal data	legal ground article 6 (1) of GDPR	purpose	place of processing	department
name Phone number email address	a) consent b) contractual egreements f) marketing	Company policy, business development, direct marketing, contractual obligations	file server protected by authorization server protected by authorization central administration office (CEO),	central administration (CEO)

Due to special situations, data process may differ from the table hereup, by providing all rights to data subjects according to personal data legislation.

Data Security (Info tv. 7.§, GDPR Article 32)

TC&C undertakes appropriate technical and organizational measures in view of the state of science and technology and the costs of implementation, the nature, scope, circumstances and objectives of data management and the risk of varying probability and severity of natural persons' rights and freedoms, to guarantee an adequate level of data security, including, inter alia, where appropriate:

a) the pseudonymization and encryption of personal data;
(b) ensuring, maintaining, integrity, availability and resilience of the continuing confidentiality of systems and services used to process personal data;
(c) in the case of a physical or technical incident, the ability to restore access to personal data and the availability of data in good time;
(d) the procedure for systematic testing, assessment and evaluation of the effectiveness of technical and organizational measures taken to ensure the security of data processing.

Rights of data subjects – application protocol (Info tv. 14.-19.§, GDPR Art 12-22.)

TC&C Informs all parties concerned about the process of their personal data and ensures that the data is processed with an appropriate legal basis. In the light of this, where the consent of the data subject is required for the processing of personal data, According to GDPR, and

other relevant legal regulations, TC&C ensures the possibility of granting or refusing consent.

1. Data subject may apply to TC&C to provide information about personal data process, request personal data correction, and request the deletion or blocking of personal information, except mandatory process.
2. At the request of the data subject, TC&C shall provide information on the data, source, purpose, legal basis, duration of processing, name and address of the data processor addresse of personal data and the legal basis of address.
3. The data controller shall provide the information in writing in the shortest possible time, at most within 30 days of the submission of the request, in an understandable form, at the request of the person concerned. Information is free of charge.
4. If personal data does not comply with reality and the personal data corresponding to reality is available to the TC&C corrects the personal data.
5. Instead of deletion, TC&C locks out personal data if the data subject so requests or if, based on the information available to him, it is assumed that the deletion would harm the legitimate interests of the data subject. Blocked personal data can only be processed as long as there is a data management porpuse that excludes the deletion of personal data. Access to the blocked personal data is restricted to the expected extent.
6. TC&C deletes personal data if its process is unlawful, the subject requests, the data is incomplete or incorrect - and this status can not be legally remedied - provided that the deletion is not excluded by law, the purpose of the data is discontinued or the statutory deadline for storing the data expired, ordered by the court or by the National Data Protection and Information Authority.
7. TC&C shall, by appropriate technical means, indicate the personal data if the subject concerned disputes its accuracy, but the incorrect or imprecise nature of the disputed personal data can not be clearly identified.
8. Correction, blocking, marking and deletion shall be notified to the data subject and all recipients. Notification may be omitted if it does not compromise the legitimate interest of the data subject in consideration of the purpose of data process.
9. If the data controller fails to comply with the relevant correction, blocking or deletion request, within 30 days of infroms the data subject in writing the factual and legal reasons for rejecting the request for rectification, blocking or cancellation. In the case of refusal of an application for rectification, dletion or blocking, the data controller shall inform the person concerned of the judicial remedy and the possibility of appeal to authorities.

Incident protocoll

1. The privacy incident shall be notified to the competent supervisory authority by TC&C without delay and, if possible, at the latest 72 hours after the data protection incident has occurred, unless the privacy incident is unlikely to pose a risk to the rights and freedom.
2. If the notification is not filed within 72 hours, the reason for the delay shall be sent together with the notification.

3. The notification of the privacy incident includes:

   (a) the nature of the privacy incident, including the categories of persons concerned and their approximate number, as well as the categories and the approximate number of data affected by the incident;
   (b) the name and contact details of the person responsible for the notification measure;
   (c) the likely consequences of a data protection incident;
   (d) measures taken or planned by TC&C to remedy the incident, including, where appropriate, measures to mitigate any adverse consequences resulting from the incident.

4. Data privacy incidents are registered by database. The updating of the register is ensured by the person responsible for data protection.

5. Informing affected persons:
   (a) If the privacy incident is likely to pose a high risk to the rights and freedoms of natural persons, TC&C informs the data subject of the data breach incident without undue delay, in particular with regard to Title III. 4 (b), (c), (d).
   b) The accuracy of information is the responsibility of the person responsible for data protection.

6. The person concerned shall not be informed if any of the following conditions are met:

(a) the data controller has implemented adequate technical and organizational protection measures and applies those measures to the data covered by the data protection incident, in particular about encryption, which makes it unrecognisable for unauthorised persons.
(b) after the data protection incident, the data controller has taken further measures to ensure that high risk for the rights and freedoms of the person concerned is no longer likely to be realized;
(c) the information would require a disproportionate effort. In such cases, the parties concerned will be informed by publicly disclosed information or other similar way.

Remedy

Data subject may object to the control of personal data if:

i. the processing or transmission of personal data is solely necessary to fulfill the legal obligation of TC&C or to enforce the legitimate interests of the Provider, Data Provider or third party, unless data process is prescribed by law;
ii. the use or transmission of personal data is done for direct business acquisition, polling or scientific research;
iii. in other cases specified by law.

1. TC&C shall examine the protest within the shortest possible time but not later than 15 days from the submission of the request, and decide on the matter of its validity and shall inform the applicant in writing. If the submission is valid, process, including further data collection and data transfer, will be terminated and locked, and every person that is involved in data controll and obliged to take action to enforce the right to protest shall be informed.

2. If the subject disagrees with the decision of TC&C, he or she may appeal to the court within 30 days from the date of its communication.
3. The data controller must demonstrate that data process is in compliance with the law. The data recipient has to prove the legality of the transfer of data.

4. Complaint against a potential infringer of the data controller may be used by the National Data Protection and Information Authority:

Authority for Data Protection and Freedom of Information
address: 22/C Szilágy Erzsébet fasor, Budapest 1125
phone: +36 -1-391-1400
email address: ugyfelszolgalat@naih.hu

Compensation (Info tv. 23. §)

1. If the data controller causes damage to by unlawful process or violation of data security requirements, damage shall be compensated.
2. If the data controller breaches personal right of the data subject by the unlawful process violating the requirements of data security, the data subject may request compensation.
3. The data controller is liable for the damage caused by the data processor to the data subject and the data controller is obliged to pay to the data subject the personal

injury violation caused by the data processor. The Data Controller is exempt from liability for damages if it proves that the is caused by an unavoidable cause outside the scope of the data processing.

4. No compensation shall be payed and no damages may be claimed in so far as the damage caused by negligence or misconduct by data subject.

Most relevant legislation

- Act CXII of 2011 on Informational Self-determination and Freedom of Information
- Act CVIII of 2001 on certain issues of electronic commerce services and information society services
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities
- Act C of 2003 on electronic communications (especially 155 §)