

# **Data protection policy**

## **2018**

**Name of the Enterprise: Club Service Kft.**

**Registered seat: 4028 Debrecen, Kassai út 83.**

**Business premises/Mailing address: 4024 Debrecen, Kossuth u. 42.**

**Name of authorised representatives: Orsolya Balogh, Tamás Balogh**

**Effective date: 25 May 2018.**

## **I. The scope of the policy**

The scope of this policy includes the whole of Club Service Kft., a company engaged in the activity of organising and managing events (hereinafter: the Enterprise), all of its employees, as well as the clients intending to participate at the conferences organised by the Enterprise and to be included in the online database of the Enterprise. The data controlling activity governed by the present policy is aimed at the data of natural persons.

Data protection officer: Krisztina Oroszné Horváth, chief financial officer, e-mail address: [clubservice@clubservice.hu](mailto:clubservice@clubservice.hu); phone number +36 30 326 4868.

## **II. The aim of the policy**

The aim of the policy is to ensure the protection of personal data in accordance with the provisions of the Fundamental Law of Hungary, the enforcement of the right of informational self-determination, and for the Enterprise to determine the rules of data protection and data security guiding its data controlling activities. A further aim of the policy is to regulate, in a comprehensive manner, the provisions concerning the controlling and occasional processing of personal data necessary for the participation at the conferences organised by Club Service Kft. and for the operation of the Regina database.

By adopting the present policy, the Enterprise undertakes compliance with the principles applicable to the controlling of personal data as prescribed by Article 5 of Regulation (EU) No 2016/679 of the European Parliament and of the Council (“GDPR”).

## **III. Definitions**

From among the terms defined in the GDPR, the following are to be emphasised in accordance with the nature of the present policy:

- a) personal data: 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.
  
- b) data controlling: 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.

- c) data controller: the natural or legal person, or company having a legal personality 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 data controller or the specific criteria for its nomination may be provided for by Union or Member State law.
  
- d) data processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.
  
- e) recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 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.
  
- f) third party: 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 data controller or data processor, are authorised to process personal data.
  
- g) filing system: any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
  
- h) 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.
  
- i) representative: natural or legal person established in the Union who, designated by the data controller or data processor in writing pursuant to Article 27 of the GDPR, represents the data controller or data processor with regard to their respective obligations under the provisions of the GDPR.

- j) enterprise: 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.

Clients intending to participate at conferences and events organised by the Enterprise and to be included in the online database of the Enterprise shall be considered as data subjects on the basis of the Information Act. The personal data provided by the data subjects shall be controlled by the Enterprise.

#### **IV. The legal basis of the data controlling**

- The Enterprise shall perform the data controlling activity lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).
- The Enterprise shall collect the personal data for specified, explicit and legitimate purposes and not further controlled in a manner that is incompatible with those purposes (purpose limitation). The clients of the Enterprise are the participants of the conferences and events organised by the Enterprise, who provide their consent to the controlling and storage of the personal data during the online registration process.
- The Enterprise shall perform the data processing in an adequate, relevant and limited way with respect to what is necessary in relation to the purposes for which they are processed (data minimisation). Accordingly, the Enterprise shall not collect or store more data than is indispensable for the realisation of the purpose of the data controlling. The Enterprise shall control the personal data recorded for the following purposes: organising conferences, operating online database, maintaining contact with clients.
- The data controlling of the Enterprise is accurate and up to date. The Enterprise shall take every reasonable step 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).
- The Enterprise shall keep the personal data 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, also with a view to retention obligation as may be prescribed by the relevant provisions of law (storage limitation). The Enterprise shall only store the personal data until the clients request the erasing of the same. Pursuant to the Information Act, in case of erasure, the data provided earlier is rendered unrecognisable in a way that they can never again be restored.

- Using appropriate technical or organisational measures, the Enterprise shall ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality).
  
- The Enterprise shall be responsible for, and be able to demonstrate compliance with the principles detailed above (accountability). In accordance with the above, the Enterprise shall ensure the continuous enforcement of the present policy, the regular revision of the data controlling activity, and if necessary, the modification and supplementation of the data controlling procedures. In order to demonstrate compliance with the legal obligations, the Enterprise shall prepare documentation.
  
- The Enterprise sets forth that it shall store the personal data controlled by it at its business premises (4024 Debrecen, Kossuth u. 42) in the form of electronic files and paper-based documents, in compliance with the legal requirements pertaining to data security.

## **V. The legal bases for data controlling**

### **The consent of the data subject:**

The lawfulness of the controlling of personal data shall be based on the consent of the data subject. The data subject may provide his/her consent to the controlling of the personal data in the following forms:

- in writing, in the form of a declaration of consent to the controlling of personal data;
- electronically, on the online registration interface operated by the Enterprise, by clearly checking a box, the data subject may consent to the controlling of his/her personal data.

The data subject may revoke his/her consent to the controlling of the personal data at any time.

### **Persons authorized to have access to the data:**

The employees of the Enterprise authorised to have access related to the relevant data controlling purpose may be able to access the personal data.

All employees of the Enterprise shall have access to the data provided by the participants in the course of registering for the conferences organised by the Enterprise.

### **The transmission of the data:**

The personal data provided in the course of registering for the conferences shall not be transmitted to any third party.

## **VI. The rights of data subjects and the enforcement of such rights**

In compliance with the provisions of the GDPR, the Enterprise shall provide information to the data subjects at any time when requested on the controlling of their personal data. Data subjects may request their personal data to be rectified or – with the exception of cases where the data controlling is required by a provisions law – erased.

In case of objections, data subjects may submit requests for legal remedies or complaints to the following authority:

National Authority for Data Protection and Freedom of Information

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Phone: +36-1-391-1400 Fax: +36 -1-391-1410

Website: [www.naih.hu](http://www.naih.hu)

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

## **VII. The handling of personal data breaches**

- A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural persons concerned.

- Personal data breaches shall be notified by the Enterprise to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

- It is not necessary to notify the supervisory authority if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

- Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

- In case it is necessary to notify the supervisory authority of the personal data breach, the notification shall:

- 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 by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Enterprise shall, without undue delay, notify the data subjects concerned of the personal data breach.
  - If the Enterprises uses a data processor, the data processing agreement shall stipulate that the data processor is required to notify the Enterprise, without any delay, of any personal data breach occurring at the data processor.

## **VIII. Data controlling activities related to employment**

### **1. Data controlling prior to employment**

Data controlling prior to the establishment of the employment relationship may occur by way of the recruitment process and the aptitude testing of the applicant for the given position.

#### **a) Data controlling during the recruiting process aimed at the hiring of employees**

- The legal basis of the recruiting process aimed at the hiring of employees is the consent of the data subject.
- The purposes of the data controlling: evaluation of application, conclusion of employment contract
- Scope of personal data concerned with the data controlling: name, address, place and date of birth, education, qualification, telephone number, e-mail address, photograph.
- Categories of persons affected by the data controlling: persons applying for a position.
- Recipients of the personal data: person exercising employer's powers, employee(s) discharging HR-related tasks, Bercontroll Audit Kft. as the company providing payroll accounting services.
- Duration of the data controlling: after the selection of the employee, the data controlling purpose ends with respect to applicants not selected, and therefore, their personal data shall be erased without delay.
- There is also an obligation to erase the personal data of the selected applicant who changes his/her mind during the recruitment process and withdraws his/her application. The applicant shall be notified on the decision made in the subject of the selection.

#### **2) Data controlling during the aptitude testing of the applicant for the given position**

- Pursuant to Section 10 (1) of the Labour Code, employees may only be requested to take two types of aptitude test: one the one hand, those prescribed by employment regulations, and on the other hand, and those that are not prescribed by employment regulations, but deemed

necessary with a view to exercising rights and discharging obligations in accordance with employment regulations.

- In case of either type of aptitude tests, detailed information shall be provided for employees concerning what skills or capabilities the aptitude test intends to assess, and what tools and methods will be used for the testing. If the aptitude test is prescribed by law, the employees shall also be informed about the title and the exact provision of law concerned.

- The legal basis for the data controlling is the employer's rightful interest.

- The purposes of the data controlling: aptitude testing to determine the suitability of the applicant for the position, establishment of the employment relationship.

- The recipients of the personal data: with respect to the results of the test, the expert administering the test and the person being tested. The employer may only receive the information whether the person tested is suitable for the given position and what conditions need to be provided. However, the employer shall not receive the details or the full documentation of the test.

- Duration of the controlling of the personal data related to the aptitude testing: 3 years after the termination of the employment.

### **3) Data controlling during the employment**

a) Data controlling in the framework of an employee register.

- The legal basis for the Enterprise controlling the employee's personal data identified below in its employee register are the basis of the rightful interest of the employer, compliance with a legal obligation, and the performance of a contract. The Enterprise shall inform the employee of the legal basis and the purpose of the data controlling prior to its commencement.

- The scope of personal data controlled by the Enterprise in the framework of the employee register

- i. name
- ii. permanent and temporary address, mailing address,
- iii. contact information, telephone number, e-mail address,
- iv. social insurance identification (TAJ) number, personal identification card number,
- v. the amount of the salary,
- vi. bank account number,
- vii. garnishments, legal title and bank accounts for garnishments,
- viii. children and other dependants, their social insurance identification (TAJ) numbers,
- ix. relative to notify in case of emergency.

- The scope of persons affected by the data controlling: the chief financial officer, the managing director and Bercontroll Audit Kft., the company performing the accounting services.

- The recipients of the personal data mentioned above: the person exercising employer's powers, employees and data processors of the Enterprise performing human resources, accounting and payroll accounting tasks.

- The purpose of the data controlling: the performance of employment related obligations, (payment of salaries), the exercise of employment related rights. Entering into and termination of employment relationship.

Duration of the data controlling: 3 years after the termination of the employment.

b) The checking of the employee's conduct related to the employment

- The employer may only check such conduct of the employee that is related to the employment relationship. The checking, as well as the tools and methods used for the same may not involve the violation of the employee's human dignity. The private life of the employee may not be checked.

- The employer shall inform the employee in advance on the use of any technical devices serving the purpose of checking the employee.

#### **4) Data processing pertaining to the use of the e-mail account made available by the Enterprise to the employee**

- The Enterprise makes an e-mail account available to the employees in order for them to maintain contact with each other, or with customers, other persons and organisations, representing the Enterprise.

#### **5) The use of laptop computer, mobile phone made available to the employee**

- The Enterprise may make "company" laptops, tablets and mobile phones available to employees in certain positions for the purpose of performing their work.

#### **6) Case-by-case data controlling pertaining to employees**

- In the interest of developing communication between the employees, facilitating more efficient communication between them, increasing their level of trust, strengthening mutual respect and commitment, the employer organises team building trainings and other events where employees are provided an opportunity to participate.

- The legal basis for the data controlling in the course of the activity mentioned above is the consent of the employee.

- The purpose of the data controlling is developing communication between the employees, facilitating more efficient communication between them, increasing their level of trust, strengthening mutual respect and commitment.

- The scope of the data subjects: all employees who participate at the trainings and other events.

- The scope of personal data: the photograph and sound recording of employees.

- Deadline for the erasure of the data: the revocation of the consent or 6 months after publication in the internal system of the employer.

- Persons entitled to have access to the data (categories of recipient): none.

#### **IX. Data controlling pertaining to the website operated by the Enterprise**

#### a) Information related to the data of visitors to the website of the Enterprise

- When visiting the website of the Enterprise, one or several cookies – small packages of information sent by the server to the browsers and then returned by the browser to the server on the occasion of each request to the server – are sent to the computer of the user, through which the browser of the user will be individually identifiable if the person visiting the website, after receiving clear and transparent information, gave his/her express (active) consent by way of further browsing the website.

- Cookies are used exclusively for the purposes of enhancing the user experience and automating the log-in process. The cookies used on the website do not store any information suitable for personal identification, and therefore, the Enterprise does not engage in the controlling of personal data in this respect.

#### b) Registration, subscribing to newsletter

- The legal basis in case of subscribing to newsletter is the consent of the data subject, which is provided on the website of the Enterprise or in the “REQUESTING INFORMATION ON PROFESSIONAL CONFERENCES” menu item on the websites of conferences and events organised by the Enterprise, by way of completing the questionnaire.

- The scope of the data controlled in case of subscribing to newsletter: name, e-mail address.

- The scope of the data controlled in case of registration: name, address, e-mail address, telephone number, place and address or work, password.

- The purpose of the data controlling in case of subscribing to newsletter: providing information to the data subject on conferences, events organised by the Enterprise.

- The recipients of the data (persons who may have access to the data) in case of subscribing to newsletter, registration: the managing director of the Enterprise, the staff member in charge of customer services, staff members of the data processor operating the website of the Enterprise.

- The duration of the data controlling in case of subscribing to newsletter, registration: until the revocation of the consent. In case of subscribing to newsletter: until unsubscribing; in case of registration: until deletion at the request of the data subject.

- The data subject may unsubscribe from the newsletter at any time or may request the deletion of his/her registration (erasure of data). Unsubscribing from the newsletter is possible by clicking on the unsubscribe link at the footer of the electronic mail sent to the data subject.

### **X. Provisions pertaining to the use of a data processor**

The Enterprise uses an external data processor with respect to the personal data controlled by it for the purposes of performing the following tasks:

- the operation and maintenance of website, online registration interface;
- the performance of tax and accounting obligations.

The rights and obligations of the data processor related to the processing of personal data are determined by the law and, within the framework of separate statutory provisions pertaining to data processing, by the data controller. The Enterprise declares that, in the course of its data processing activity, the data processor may not make any substantial decision affecting the data control, that it may only process the personal data in its possession in accordance with the data controller’s instructions, that it may perform no data processing for its own purposes,

and that shall store and retain the personal data processed as required by the data controller. The Enterprise does not authorise the data processor to engage sub-processors. A written contract shall be concluded for the data processing activity. No entity may be put in charge of the data processing when such entity is interested in business activities using the personal data to be processed.

#### **XI. Implementing and closing provisions**

The present policy shall enter into effect on 25 May 2018.

The managing director shall be required to inform all employees of the Enterprise of the provisions of the present policy. The managing director of the Enterprise shall ensure that all employees of the Enterprise comply with the provisions of the present policy. For the purpose of performing this obligation, the managing director of the Enterprise shall prescribe that the employment contracts with the employees be amended in such a way that the employees' undertaking of obligation to comply with and enforce the present policy is declared.

The adoption and amendment of the present policy shall belong to the scope of tasks of the managing director of the Enterprise.

Date: 18 May 2018

Club Service Ltd.