SPRINGTAB APPLICATION

PRIVACY POLICY AND DATA CONTROL GUIDELINES

1. Introduction

The aim of the current Regulation is to declare the data handling and control guidelines of the data controller of SpringTab (further: Application), SpringTab Szolgáltató és Fejlesztő Korlátolt Felelősségű Társaság (further: Company) and the data protection and handling policy, all of which the Company recognizes as compulsory. In establishing these guidelines, the Company recognized especially the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing, Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities guidelines, together with "Online Privacy Alliance" guidelines.

The aim of the current Regulation is to assure that the services offered by the Company, for every individual, irrespective of nationality or domicile, that during the handling of her data, her rights and fundamental freedoms are respected, especially her right for private life (data protection).

Controller reserves the right to alter the current Policy at any time.

In case users have doubts about guidelines that are unclear from the current Regulation, please get in touch and our colleagues will answer your query.

Controller is committed to the protection of personal data of its partners and users, respects informational self-determination of its users, handles private data confidentially, and does all measures in terms of security, technology and organization that guarantees security of data.

Name of data controller: SpringTab Szolgáltató és Fejlesztő Korlátolt Felelősségű Társaság

Address: 1146 Budapest, Hermina út 5. fszt. 2.

Data control identification number: **NAIH-78535**

2. Definition of notions regarding data policy

‘personal data’ shall mean any information relating to the data subject, in particular by reference to his name, an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, and any reference drawn from such information pertaining to the data subject;

‘the data subject’s consent’ means any freely and expressly given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed without limitation or with regard to specific operations;

‘the data subject’s objection’ shall mean an indication of his wishes by which the data subject objects to the processing of his personal data and requests that the processing of data relating to him be terminated and/or the processed data be deleted;

‘controller’ shall mean the natural or legal person, or unincorporated body which alone or jointly with others determines the purposes of the processing of data, makes decisions regarding data processing (including the means) and implements such decisions itself or engages a data processor to execute them;

‘processing of data’ shall mean any operation or set of operations that is performed upon data, whether or not by automatic means, such as in particular collection, recording, organization, storage, adaptation or alteration, use, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and blocking them from further use, photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images);

‘disclosure by transmission’ shall mean making data available to a specific third party;

‘public disclosure’ shall mean making data available to the general public;

‘erasure of data’ shall mean the destruction or elimination of data sufficient to make them irretrievable;

‘blocking of data’ shall mean the marking of stored data with the aim of limiting their processing in future permanently or for a predetermined period;

‘**destruction of data’** shall mean the complete physical destruction of the medium containing data;

‘**third party’** shall mean any natural or legal person or unincorporated organization other than the data subject, the controller or the processor;

3. The controlled private data

The user, at her own will, connects her Facebook account with the Application. In this case, Company is entitled to handle the following data: Facebook name, email address, profile picture, gender, friend list, location, birth date and place.

Moreover, it can handle all data, which user publishes, with acceptance of Facebook’s Privacy Policy, to others. Especially those that the user shares on Facebook, or specifies during activity on Facebook, such as adding a friend, liking a page, importing contacts or changing her relationship status.

User can decide not to connect its account with the Application. In this case, upon decision of the user, Company can handle the following data: email address, name, nick name, address, location. User has the option to share additional data.

4. Plea of data control, guidelines during data control

Data control will occur upon the user’s declaration, which is voluntary, and based on adequate information. This declaration contains the user’s explicit consent that during the

usage of the page, data that she granted access to, as well as data generated about her, will be used. The plea of the data control is explicit consent according to Art. 5, Section 1 a) of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

The aim of the handling of the recorded data is publishing personalized content and advertisements, statistics, development of the IT system, protection of user rights. Data shared by users during the usage of the service can be used by the Company with the aim to construct user groups, and to show them targeted content and/or advertisements on websites that use the Application.

Controller is not allowed to use data for aims other than described above. It is also set forth in this Regulation that data transfer between Controller and its partners can be done without separate consent. Sharing of personal data to third party or authority – unless explicit law requires it – is permissible only upon resolution by an authority or with explicit and prior consent by the user.

Controller does not check personal data controlled. The person who shared the data is responsible for its validity.

Controller places a "cookie" (small piece of data) on the computer of the user, in order that personalization is possible. With the usage of the Application, the user accepts the placement of cookies on her computer.

Controller, acting as technological provider, can ensure that, during the usage of the Application or visit of a partner website, partners of Controller, especially Google Inc. store, with the help of cookies, any prior visit and that they show advertisements.

The cookie can be deleted from the user's computer, and also set her web browser to block the usage of them. Furthermore, Google Inc. ensures that the user can disable cookies on the website designed for that purpose (http://www.google.hu/privacy_ads.html). Blocking of cookies can potentially cause websites to become less comfortable for the user.

Visitors of websites using the Application can decide voluntarily to subscribe to the newsletter of the Controller or its partners that contain additional information and will be sent periodically.

When registering for the newsletter, the user should specify her valid email address.

Controller is allowed to use this piece of data for the sole purpose of sending the newsletter, it does not connect this piece of data with any other piece of data, nor use it for any other purpose, or forward it to third parties.

In case the user unsubscribes from the newsletter, Controller deletes its email address immediately and irrevocably.

We let the user know that the court, the prosecutor or the investigating authority can contact the Controller, for the purpose of information, data transmission, or making available documents. In this case Controller, for the authorities, when the respective authority specified the exact aim and scope of the data, shares personal data to the extent that is absolutely essential for the purposes of the investigation.

We give further notice about data control not listed in this policy at the point of data record.

5. Principles of data control

Data should be acquired and recorded only lawfully and fairly.

Data can be stored only for the specified aim and it cannot be used for other purposes.

Data stored should be in proportion with the aim of their storage and should comply with their purpose, they cannot overreach this aim.

Certain measures shall be done in order that data stored in automatized databases are protected against involuntary or unlawful destruction, accidental loss, unauthorized access, change or distribution.

6. Privacy policy measures applied by the Company

The Company uses private data that are essential for the usage of the Company's services upon approval of the concerned users and only for purposes specified.

The Company, as Controller, undertakes that it will treat data acquired in accordance with provisions set forth in Infotv. and data protection principles set forth in the current Regulation and it does not transfer data to third parties.

An exception from the measures set forth in this part is usage of data in a statistically summarized form which does not contain the name of the user, or any other information from which the user can be identified. Thus, this process is not considered Data Control or Data Transfer.

The Company, in certain cases – official contact by the court or police, legal proceedings due to copyright, property right or other infringement, or their reasonable suspicion, with the aim of prejudicing the interests of the Company, or imperiling the services of the Company, etc. – makes data concerning the user available for third parties.

The system of the Company can gather data about the activity of the user, data that cannot be connected with data given by the user at the time of registration, nor with data generated by visiting other websites or using other services.

The user should be informed about the aim of Data Control and about who treats or processes their data. Information about Data Control is considered adequate when a law rules about existing Data Control – data record by means of forwarding or connecting.

Each case when the Company intends to use data for purposes other than that was specified at the initial data record, it informs the User and receives her explicit consent, or provides her with the opportunity to deny usage.

The Company, as Controller, respects the regarding limitations set forth by the law at data input, record, and management.

The Company obliges itself that it applies care with the security of the data, does all the necessary measures in terms of technology and organization, and establishes the rules of procedure that ensure security of data recorded and prevent them from loss, unauthorized use and unauthorized modification. It also obliges itself that it will inform all third parties to whom data may be transferred to respect its duties.

Controller locks personal data when the concerned user requests it, or when information available indicates that deletion would harm the lawful interests of the user. Personal data locked this way may only be treated insofar as the data control aim, which excluded deletion of personal data, persists.

The concerned User, together with all to whom data was transferred, must be notified about correction, or deletion of her data. Notification may be omitted in case this does not harm lawful interest of the concerned user with respect to the aim of Data Control.

7. Duration of data control

Control of Personal data specified by the User will pertain as long as the User unsubscribes – with its username – and at the same time requests deletion of her data. The deadline for deletion is 10 working days from the receipt of the User's request. In this case, data will be deleted from all Controllers defined in the current Regulation.

In case of unlawful, misleading use of Personal data, crime committed by the User, or attack against the system, Controller is authorized to delete the registration of the User and at the same time delete all her data. Nevertheless, in case of suspected criminal responsibility or civil responsibility, Controller is authorized to keep the data for the duration of the proceedings.

Personal data provided by the User – also in case the User does not unsubscribe from the service or with deletion of her registration does not terminate rights for her data, her stored comments and uploaded content stays – can be controlled by the Company, as Controller, as long as User does not request explicitly, in written form, termination of control. The User's

request to terminate Control without unsubscribing from the service does not affect her right to use the service, but she might not be able to use certain services without Personal data. Data is deleted within 10 working days from the receipt of request.

Data stored automatically during functioning of the system are stored from their generation to a certain period that ensures safe functioning of the system. The Company ensures that these automatically recorded pieces of data cannot be connected with other personal data – except in cases where the law provides otherwise. In case the User terminates her consent to the Control of her Personal data, or unsubscribes from the service, then she may not be identified from technical data – except for investigating authorities and their experts.

8. Third party service providers

The Company – during the use of some of its services – can cooperate with service providers that make registration and login easier (For example, Facebook Inc., Google Inc., further: Third party providers). With respect to systems of Third party providers, for data provided in their systems, their privacy policies are authoritative.

Regarding data made available on certain social media platforms, Data Controller is the Third party provider that makes possible sharing of content, its service is governed by its own terms of use and privacy policy.

The Company is allowed to transfer, with the aim of providing its service, certain pieces of data specified by the user to Third party providers, but the transferred data should be used for purposes specified in the current Regulation.

9. Opportunity for data transfer

The Company, as Controller is entitled and required to transfer all Personal data in its custody to the respective authorities upon law or official obligation. Controller cannot be held responsible for Such Data transfer and its consequences.

The Company keeps, for the examination of the lawfulness of such Data transfer and for the information of concerned individuals, a data transfer register.

10. Knowability of data, rights of concerned individuals, remedies

Concerned individuals may request information about the control of their personal data, and they may request correction and – except when the law provides otherwise – deletion of their personal data.

Upon request of concerned individuals Controller gives information about data controlled by the Controller or data processor appointed by the Controller, aim of data control, plea of data control, time frame of data control, name, address and headquarters of data controller, about any activity connected to data control, and about who and for what aim received

data. Controller gives information in written form that is easy to understand, at the earliest possible time, but within 30 days. This information is free of charge in case the requesting individual has not submitted request concerning the same area in the current year. In all other cases, Controller specifies a fee for this service.

Controller deletes the personal data when its control is unlawful, the concerned individual requests it, the aim of data control ceased to exist, the legal deadline of data storage passed, and when a court or data protection authority ruled so.

Controller notifies the concerned individual and others who have previously received data for data control about correction and deletion. Notice may be omitted when it does not harm the lawful interest of the concerned individual with respect to the aim of data control.

Concerned individual may protest against control of her personal data in case:

control (transfer) of personal data is required only for pursuing rights or lawful interests of data controller or data receiver, except when data control was required by law;

use or transfer of personal data pertains due to direct business purposes, poll or scientific research

law grants the opportunity to protest

Controller examines the protest – at the same time suspending data control – at the earliest from submission of the request, but within 15 days, and it notifies the requesting party about the result in written form. In case the protest is justified, controller suspends data control – including data record and data transfer – blocks data, and notifies all parties who have received personal data concerned with the protest about actions taken upon the protest, and who are obliged to take action in order to validate the protest.

In case concerned individual does not agree with the decision of the Controller, it can pursue the matter in court, within 30 days from the notification about the decision.

In case rights of concerned individual are breached, she can pursue the matter in court. The court rules in the matter out of turn.

Controller compensates damage resulting from the unlawful control of data of concerned individual or from breach of technical data protection requirements. Controller is exempt from compensation when damage was caused by unavoidable circumstances out of the reach of data control.

Damages may not be compensated in case they resulted from intentional or seriously negligent behavior of the harmed individual.

Complaints concerning data control shall be addressed to the court or the Hungarian National Authority for Data Protection and Freedom of Information.

Headquarters: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Address: 1534 Budapest, Pf.: 834
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu