TRUSTCHAIN SYSTEMS Korlátolt Felelősségű Társaság
Registered office: H-1136, Pannónia street 52. building A. 1st floor 2nd door
Registered business number: 01 09 294941
VAT number: 25895308-2-41
NAIH id: NAIH-129148/2017

DATA PROTECTION POLICY

This Policy states the data protection and management principles that the operator of www.trustchain.systems website (thereinafter: Website), the TRUSTCHAIN SYSTEMS Korlátolt Felelősségű Társaság (thereinafter: Operator) applies and agrees to be bound by.

The goal of this Policy is to ensure the rights to privacy and the protection of personal data on equal terms to all users during the services provided by the Operator.

This policy was written in view of the following Articles

- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information
- Act VI of 1998 on the Protection of Individuals with regards to the Automatic Processing of Personal Data, on the publishing of Agreement of 28/01/1981 in Strasbourg
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities.

1. Definitions

1.1 Personal data: any data, which is related to an identified natural person, and able to make conclusions about the person based on the data. Personal data shall be considered as such until its relation to the person can be recovered.
1.2 Data management: any operation or set of operations which is performed on personal data, such as collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, blocking, erasing or destructing the data.
1.3 Data controller: TRUSTCHAIN SYSTEMS Korlátolt Felelősségű Társaság (LLC.) (Operator)
1.4 Processing of data: any act of data management operations, regardless of methods, equipment and place, as long as the operation is carried out on the data.
1.5 Destruction of data: complete physical destruction of the equipment containing the data
1.6 Transmission of data: making the data accessible to determined third parties
1.7 Disclosure: the data is made accessible to anyone
1.8 Deletion of data: making the data unrecognisable in a way that it cannot be recovered
1.9 Automatic processing: includes the following operations if done completely or partly with automatized equipment: storage of data, logical or arithmetic operations done on the data, modification, deletion, retrieval or disclosure of data

2. Managed personal data

2.1 The following types of data are managed by the Operator:

- email address,
- name (family and first name).

2.2 These data are given by the User via registering for the service.

3. Additional data

3.1 The Operator places a small data package (so called 'cookie') on the computer of the user for a personalized service. The purpose of the cookie is to ensure the highest quality operation of the Website. The user is able to delete the cookie from his own computer or he can adjust the browser to block the application of cookies. By blocking the application of cookies, the user acknowledges that the operation of the Website is not the same quality without the cookie.

4. Legal basis of data management

4.1 The legal basis of data management is provided by the voluntary statement of the User, which is given after the Operator's proper communication of information.

5. Newsletter and electronic advertisement service - as the purpose of data management

5.1 If the user subscribe for the newsletter and electronic advertisement service, the Operator manages data to send newsletters and electronic advertisements - about promoting the services offered by the Operator or containing informative messages related to the activity fields of the Operator - to the user, regularly via e-mail, which may contain direct marketing messages in the interest of the Operator, or promoting the services of the Operator. The user can unsubscribe any time by using the unsubscribe link in the bottom of every newsletter, or by any other way detailed in chapter 8-9.

5.2 The Operator uses a separate external data processor who provides the technical background by an automated system:

Name: SendGrid Ltd.
Registered seat: 1801 California Street, 1801 California St, Denver, CO 80202
Dataprocessing: 1801 California Street, 1801 California St, Denver, CO 80202
Contact: SendGrid Customer Support, support@sendgrid.com

5.3 The Data are managed until Operator receives the request of the user for unsubscribe from the service or the request for the deletion of the data, but for a maximum of 5 years.

5.4 The Operator shall not use the personal data for other purposes than those mentioned in section 5. The transmission of personal data to third parties or authorities, is only possible -

except where compulsory by law - with a court or authority decision or with the prior, explicit consent of the User.

5.5 The data, which collected for statistical utilisation purposes are collected in a format, which does not include the User's name or other data. This type of data can not be used for identification in any form, thus it does not qualify neither as data management nor as data transmission.

6. Responsibility

6.1 The Operator does not check the provided personal data. Only the person providing the data is liable for the compliance of the provided data.

6.2 Any User providing his email address, at the same time, shall assume responsibility for him being the only person who accesses services from that email address. Regarding this responsibility, the user who registered the email address, is liable for all responsibility related to logging in with the given email address.

7. Data Protection Principles

7.1 It is the Operator's priority to ensure the protection of the user’s rights.

7.2 Data shall only be collected, stored and utilised for purposes given in this Policy and for purposes allowed by law.

7.3 Data can only be managed with the appropriate legal basis, fairly and lawfully.

7.4 The nature and amount of data stored have to be proportionate to their utilisation goal, and have to be appropriate for the goals outlined in this Policy and shall not be used for other purposes.

7.5 The Operator shall do every safety measure to protect the personal data stored in the automated data set, against accidental or purposeful deletion, accidental loss, unlawful access, disclosure, modification and transmission.

7.6 The Operator keeps a register of data protection in order to check the legality of data management and to facilitate communication of information.

8. Access to personal data

8.1 The Operator is entitled to manage the data provided by the user, unless the user eliminates his approval to the management of his personal data in the following methods; the user is also entitled to correct, modify data provided by himself:

- requests the deletion or modification of his personal data in e-mail, sent to admin@trustchain.systems, exclusively from the email address that he provided
- requests the deletion or modification of his personal data in written form, sent to Operator’s postal address (H-1136, Pannónia street 52. building A. 1st floor 2nd

door), in this case it is necessary to verify the identity of the user and the relationship to the data.

The deletion of data shall be made within 30 days from the day of receipt of the user's demand for deletion.

8.2 By way of derogation from 8.1, the Operator is entitled to continue utilising the data in case it is needed to fulfil its legal obligations, as long and as much as stated by legal provision.

8.3 Operator blocks the personal data if the user requests this by the methods detailed in point 8.1 or in case it can be suspected - based on the available information - that the deletion would harm the legitimate interests of the user. Thus blocked personal data shall only be managed as long as it is necessary for the data management goal, which excludes the deletion of the data.

8.4 The user and all other parties, who previously received the lawfully transmitted data, have to be notified of the corrected, deleted or blocked data. The notification may be omitted in case it does not harm the legitimate interests of the user in view of the purpose of data management.

9. Protest against the handling of personal data

9.1 Users may protest against the handling of their personal data in letter, sent to the postal address of the Operator (H-1136, Pannónia street 52. building A. 1st floor 2nd door), or in email sent to admin@trustchain.systems. The protest against the handling of personal data sent through postal service is deemed authentic if based on the sent document the user can be undoubtedly identified. The protest against the handling of personal data sent in email is deemed authentic if it is sent from the user's registered email address.

9.2 The Operator shall reply within 15 days from the day of receipt of the user's protest against the handling of personal data. In case of email the day of receipt shall be considered the first working day after it was sent.

10. Communication of Information

10.1 Users may request information about the management of their personal data from the Operator as data controller, in letter, sent to the postal address of the Operator (H-1136, Pannónia street 52. building A. 1st floor 2nd door), or in email sent to admin@trustchain.systems. The request for information sent through postal service is deemed authentic if based on the sent request the user can be undoubtedly identified. The request for information sent in email is deemed authentic if it is sent from the user's registered email address.

10.2 The request for information can include the user's data managed by the Operator, its sources, the goal of data management, its legal basis, duration, the names and addresses of

possible data controllers, activities related to data management and, in case of transmission of personal data, to who and for what purposes they get or got the data of the user.

10.3 The Operator shall reply within 25 days from the day of receipt of the User's request for information about data management. In case of email the day of receipt shall be considered the first working day after it was sent.

11. Compulsory data transmission

11.1 The Operator as data controller, is entitled and obliged to transmit all available and properly stored personal data to competent authorities, which he is obliged by the law or by enforcing compulsory order. The Operator shall not be held liable for such data transmission and consequences resulting from it.

12. Law enforcement opportunities

12.1 The user may exercise his law enforcement opportunities before court, based on Infotv. and Act V of 2013 (Civil Code), the trial would be a matter for the competent regional court.

12.2 The user may request help from, or may notify the Hungarian National Authority for Data Protection and Freedom of Information (NAIH, address:1125 Budapest Szilágyi Erzsébet fasor 22/C; postal address: 1530 Budapest, Pf. 5.; phone: + 36-1/391-1400; fax: + 36-1/391-1410, e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu) about the violation of rights related to personal data from.

12.3 NAIH identification number: NAIH-129148/2017.

12.4. The colleagues of the Operator are available for any question, observation about data management on admin@trustchain.systems email address.