

## ***PRIVACY POLICY***

<b>Document</b>	<b>Enters into force</b>	<b>Valid</b>
Data Management and Privacy Policy for Kvery.io System	2021.10.01.	until revoked



## **DATA MANAGEMENT AND PRIVACY POLICY FOR KVERY.IO SYSTEM**

**Kolt Systems Kft.** (4551 Nyíregyháza, Élet utca 25. Company registration number: 15-09-088039, Tax number: 28966717-2-15, Contact: [info@kvery.io](mailto:info@kvery.io), Phone: +36 30 468 9255, hereinafter referred to as: **service provider, data controller, data processor**) in the document containing the General Terms and Conditions for the present data processing and the provision of the service (hereinafter referred to as: GTC) undertakes to comply with the applicable data protection legislation, in particular 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 movement of such data, and repealing Regulation (EC) No 95/46/EC (hereinafter: the Regulation), Regulation (EU) No CXII of 2001 on the right to information and freedom of information (hereinafter: Infotv.) and Act CVIII of 2001 on certain aspects of electronic commerce services and information society services (hereinafter: Elker tv.) - when handling, processing and storing personal data of the Customer (hereinafter: data subject, user, Customer).

### **1. Concepts**

*Service provider* Kolt-Systems Kft. a company registered in Hungary, which provides the services of the Kvery.io system owned by Kolt-Systems Kft.

*Service provider, data controller:*

Name: Kolt Systems Kft.  
Registered address: 4551 Nyíregyháza, Élet utca 25.  
Company registration number: 15-09-088039,  
Tax number: 28966717-2-15

Complaint handling location, address for correspondence: 1095 Budapest,  
Lechner Ödön fasor 2. B ép. 7. floor. 13  
Email: [info@kvery.io](mailto:info@kvery.io)  
Phone: +36 30 468 9255

*Customer:* "Customer" refers to the person or entity ordering or subscribing to the Kvery.io Products or services by making a registration on [www.Kvery.io](http://www.Kvery.io) and subscribing to one of the available packages. as the contracting party of Kvery.io

*User:* an individual who, in his/her own name, registers at [www.kvery.io](http://www.kvery.io) into the Kvery.io system owned by the Service Provider.



*Party, Parties:* the Service Provider and the Customer, each Party, collectively: the Parties

*Service:* by accepting these General Terms and Conditions and registering in the Kvery.io administration system, the Customer enters into a contractual relationship with the Service Provider. The Customer will then parameterise the Kvery.io system according to his individual needs and use Kvery.io database related services.

*How to use the Service:* by registering and using the Kvery.io system operated by the Service Provider.

## **2. Definitions based on the Information Act and the Regulation**

*Data subject:* any natural person who is identified or can be identified, directly or indirectly, on the basis of specific personal data;

*Personal Data:* 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, 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;

*Consent:* a voluntary and explicit indication of the data subject's wishes, based on appropriate information, by which he or she gives his or her unambiguous consent to the processing of personal data concerning him or her, whether in full or in relation to specific operations;

*Objection:* a statement by the data subject objecting to the processing of his or her personal data and requesting the cessation of the processing or the deletion of the processed data;

*Data controller:* the natural or legal person or unincorporated body which, alone or jointly with others, determines the purposes for which the data are to be processed, takes and implements decisions regarding the processing (including the means used) or has them implemented by a processor;

*Data processing:* any operation or set of operations which is performed upon data, regardless of the procedure used, in particular any collection, recording, recording, organisation, storage, alteration, use, retrieval, disclosure, transmission, alignment or combination, blocking, erasure or destruction of data, prevention of their further use, taking of photographs, sound recordings or images and physical features which can be used to identify a person (e.g. fingerprints, palm prints, DNA samples, iris scans);

*Transfer:* making data available to a specified third party;



*Disclosure:* making the data available to anyone;

*Data erasure:* making data unrecognisable in such a way that it is no longer possible to recover it;

*Data marking:* the marking of data with an identification mark to distinguish it;

*Data blocking:* the marking of data with an identifier in order to limit its further processing permanently or for a limited period of time;

*Data destruction:* the complete physical destruction of the medium containing the data;

*Data processing:* the performance of technical tasks related to data processing operations, irrespective of the method and means used to perform the operations and the place of application, provided that the technical task is performed on the data;

*Data processor:* a natural or legal person or unincorporated body which processes data on the basis of a contract, including a contract concluded pursuant to a legal provision;

*Data set:* the set of data managed in a single register;

*Third party:* a natural or legal person or unincorporated body other than the data subject, the controller or the processor;

*Data breach:* unlawful processing or handling of personal data, in particular unauthorised access, alteration, disclosure, transmission, disclosure, erasure or destruction, accidental destruction or accidental damage.

### **3. Purpose of data processing, data security**

1. The Service Provider will process and store the personal information of the users in the context of the service provided to the Customers in order to provide the service and only to the extent and for the duration strictly necessary and indispensable for the provision of the service.
2. The Service Provider only processes personal data that is necessary for the purpose of data processing and is suitable for achieving the purpose.
3. The personal data will retain this quality during the processing as long as the relationship with the data subject can be re-established. The link with the data subject can be re-established if the controller has the technical conditions necessary for the re-establishment.



4. The Data Controller shall not disclose the personal data of the data subject to third parties, except to the Customer and to the intermediaries and processors specifically mentioned in this Privacy Policy.
5. The data controller shall design and implement the processing operations in such a way as to ensure the protection of the privacy of the data subjects when applying the Data Protection Act and other rules applicable to data processing.
6. The data controller or the data processor shall ensure the security of the data, and shall take the technical and organisational measures and establish the procedural rules necessary to enforce the Infotv. and other data protection and confidentiality rules. In particular, appropriate measures shall be taken to protect the data against unauthorised access, alteration, disclosure, disclosure, deletion or destruction, accidental destruction or damage and against inaccessibility resulting from changes in the technology used. In order to protect the electronically managed data files in the different registers, appropriate technical arrangements should be in place to ensure that data stored in the registers cannot be directly linked and attributed to the data subject, except where permitted by law.
7. When processing personal data by automated means, the controller and the processor shall take additional measures to ensure that.
  - a. prevent unauthorised data entry;
  - b. preventing the use of automated data processing systems by unauthorised persons using data transmission equipment;
  - c. the verifiability and ascertainability of the bodies to which personal data have been or may be transmitted using data transmission equipment;
  - d. the verifiability and ascertainability of which personal data have been entered into automated data processing systems, when and by whom;
  - e. the recoverability of the installed systems in the event of a failure, and
  - f. errors in automated processing are reported.
8. The controller and the processor shall take into account the technological development of the system when defining and implementing measures to ensure data security. It shall choose among several possible processing solutions the one which ensures a higher level of protection of personal data, unless this would impose a disproportionate burden on the controller.



#### **4. Legal basis for processing, consent**

1. The data controller informs the data subject that, in accordance with the Info. According to Article 5 (1), personal data may be processed if
  - a. with the consent of the data subject, or
  - b. it is required by law or, on the basis of the authorisation granted by law and within the scope specified therein, by a decree of a local authority for a purpose in the public interest (hereinafter: mandatory processing).
2. The communication of the data subject's/user's personal and health data to the service provider (and the service provider's Customer) and his/her consent to the processing is based on the data subject's voluntary written consent.
3. Personal data, including health data, may also be processed where obtaining the data subject's consent would be impossible or would involve disproportionate costs and the processing of the personal data would.
  - a. necessary for compliance with a legal obligation to which the controller is subject; or
  - b. is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, and the pursuit of those interests is proportionate to the restriction of the right to the protection of personal data.
4. Where the data subject is unable to give his or her consent due to incapacity or for other reasons beyond his or her control, the personal data of the data subject may be processed to the extent necessary to protect his or her vital interests or those of another person or to prevent or protect against imminent danger to life, limb or property of a person, as long as the obstacles to consent persist.
5. The consent of the legal representative of a minor over the age of 16 is not required for the validity of the declaration of consent of the data subject.
6. If the personal data have been collected with the consent of the data subject, the controller shall, unless otherwise provided by law,
  - a. to comply with a legal obligation to which it is subject, or
  - b. for the purposes of the legitimate interests pursued by the controller or by a third party, where such interests are proportionate to the restriction of the right to the protection of personal data



without any further specific consent and even after the withdrawal of the data subject's consent.

7. In judicial or administrative proceedings initiated at the request or initiative of the data subject, the data subject shall be presumed to have given his or her consent to the processing of personal data necessary for the purposes of the proceedings, and in other proceedings initiated at the request of the data subject, to the processing of personal data provided by him or her.

## **5. Information on data management and processing**

With regard to the processing of data, the Service Provider shall inform the Customer of the following with regard to the provisions of Article 10 of the Data Protection Act:

1. The rights and obligations of the data processor in relation to the processing of personal data are determined by the data processing service provider Kolt-Systems Kft. within the framework of the Infotv. and the separate laws on data processing. The data controller shall be responsible for the lawfulness of the instructions given by it.
2. The processor may use an additional processor at the discretion of the controller. The processor shall not take any substantive decision concerning the processing, shall process the personal data of which it becomes aware only in accordance with the controller's instructions, shall not process the personal data for its own purposes and shall store and retain the personal data in accordance with the controller's instructions.
3. Subject to the condition set out in Article 20(4) of the Info Act - where personal information of the data subject would be impossible or would entail disproportionate costs, as in the case of this website - the controller shall also inform the data subject of the processing prior to the data subject's consent by providing (disclosing) the following information:
  - a. *Fact of data collection, scope of data processed:* password, first and last name, e-mail address, IP address at the time of registration,
  - b. *Data subjects:* all data subjects registered in the app or on the website.
  - c. *Purpose of data collection:* the service provider processes the personal data of the Users for the purpose of the full use of the website, e.g. to
  - d. *Duration of data processing, deadline for deletion of data:* immediately upon cancellation of registration. Except for accounting documents. Pursuant to Article 169(2) of Act C of 2000 on Accounting, accounting



documents (including general ledger accounts, analytical and detailed records) directly and indirectly supporting the accounting accounts must be kept for at least 8 years in a legible form, retrievable by reference to the accounting records.

- e. *Potential data controllers who may have access to the data:* personal data may be processed by the controller's staff, in compliance with the principles set out above.
- f. *Description of the data subjects' rights in relation to data processing:* the following data can be modified on the websites: password, first and last name, e-mail address,
- g. *The data subject may request the deletion or modification of personal data in the following ways:* by post to 1095 Budapest, Lechner Ödön fasor 2. B building. 7. floor. 713., by e-mail to [info@kvery.io](mailto:info@kvery.io) .

4. The data of the data processor (hosting provider) used for the processing:

**Server4You - Host Europe GmbH**

Address:, Hansestr. 111, 51149 Cologne, Germany

VAT ID: DE187370678

Telephone: +49 221 4291 4310

Contact: [info@server4you.net](mailto:info@server4you.net)

Website: <https://www.server4you.net/legal-notice>

## **6. Management of the website cookie**

- 1. The website does not use cookies. We use HTML5 Local Storage on our websites for better functionality. With this solution, the web application stores the data locally, in the user's browser, and the information is not sent to our servers.
- 2. The Service Provider and the Customer measure the traffic data of the websites and the mobile application by using the Google Analytics service. When using this service, data is transmitted which cannot be used to identify the data subject. More information about Google's privacy policy can be found here: <http://www.google.hu/policies/privacy/ads>





## **7. Data transmission**

1. The purpose of the Kvery.io system's data transfer activity is to transfer the User's data to the Customer in order to inform the Customer about the User's subscription and to contact the User for the purpose of the service provided by the Customer.
2. The service provider aims to process online payments but does not transfer any personal data to the payment processor (Stripe - [www.stripe.com](http://www.stripe.com)) Any personal data given to process payment is not handled by the Service provider.
3. Service Provider processes personal data of the Customer's billing address. This data is received by the Service Provider from the payment provider (Stripe - [www.stripe.com](http://www.stripe.com)) and transferred to the invoice system provider KBOSS.hu Ltd. Service Provider does not store any billing data.
4. I acknowledge that the website of **Kolt Systems Kft.** (4551 Nyíregyháza, Élet utca 25. Company registration number: 15-09-088039, Tax number: 28966717-2-15, Contact: [info@kvery.io](mailto:info@kvery.io), Phone: +36 30 468 9255), [www.kvery.io](http://www.kvery.io) will transfer my billing data includes: name, billing address, e-mail address, phone number, tax number to KBOSS. hu Ltd. Purpose of the data transfer: to carry out the invoicing of the subscription fee.
5. The personal data transferred may be processed by the following, in compliance with the above principles:

### **KBOSS.hu Ltd.**

Registered office: 1031 Budapest, Záhony utca 7.

Company registration number: 01-09-303201

Tax number: 13421739-2-41

E-mail: [info@szamlazz.hu](mailto:info@szamlazz.hu)

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

## **8. Customer relations and other data management**

1. Should the data controller have any questions or problems when using our services, the data subject can contact the data controller via the methods provided on the website and mobile application (phone, e-mail, social networking sites, etc.)



## **9. Data security**

1. The controller shall design and implement the processing operations in such a way as to ensure the protection of the privacy of data subjects. The data controller shall ensure the security of the data (password and anti-virus protection), take the technical and organisational measures and establish the procedural rules necessary to enforce the Info Act and other data protection and confidentiality rules.

## **10. Data processor**

1. The data controller uses the following data processor for the operation of the website and application:

**Kolt Systems Kft.**

Registered address: 4551 Nyíregyháza, Élet utca 25.

Company registration number: 15-09-088039,

Tax number: 28966717-2-15

Email: [info@kvery.io](mailto:info@kvery.io)

Phone: +36 30 468 9255

## **11. Obligations and rights of data subjects**

1. *Providing real data:* the data subject is obliged to provide real data when providing his/her data. If the personal data is not accurate and the accurate personal data is available to the controller, the controller shall correct the personal data (the latter is found in Article 17 of the Info law). Kolt-Systems Kft. and its data processing Customer and employee exclude any liability for the consequences of providing data that is not true.
2. *Request for information:* Pursuant to Article 14 of the Info Act, the data subject has the right to request the controller to provide information on the processing of his or her personal data, and may also request the rectification, erasure or blocking of his or her personal data. According to Article 15. the controller shall, upon request of the data subject, provide information on the data of the data subject processed by the controller or by a processor appointed by the controller or under the controller's instructions, on the source of the data, the purpose, legal basis and duration of the processing, the name and address of the processor and the activities of the processor in relation to the processing, the circumstances and effects of the personal data breach and the measures taken to remedy the data breach, and, in the event of the transfer of the data subject's personal data, the legal basis and the recipient of the data transfer. The controller shall provide the information in writing, in an intelligible form



and at the data subject's request, within a minimum of 25 days from the date of the request.

3. *Refusal to provide information:* the data controller may refuse to provide information to the data subject only in the cases specified in Article 9(1) and Article 19 of the Info.tv. In the case of refusal to provide information, the controller shall inform the data subject in writing of the provision of the Info. law on the basis of which the refusal to provide information was made. In the case of refusal to provide information, the controller shall inform the data subject of the possibility of judicial remedy and of recourse to the National Authority for Data Protection and Freedom of Information (hereinafter referred to as the Authority).
4. *Deletion of data:* personal data will be deleted by the Service provider in the following cases:
  - a. if its treatment is unlawful;
  - b. the data subject requests - in accordance with point (c) of Article 14 of the Data Protection Act;
  - c. it is incomplete or incorrect - and this condition cannot be lawfully remedied - provided that deletion is not precluded by law;
  - d. the purpose of the processing has ceased or the statutory time limit for storing the data has expired;
  - e. ordered by a court or the Authority.
5. *Blocking of data:* instead of erasure, the controller will block personal data if:
  - a. the data subject so requests, or
  - b. if, on the basis of the information available to it, it is likely that the erasure would harm the legitimate interests of the data subject.

The personal data blocked in this way may be processed only for as long as the processing purpose that precluded the deletion of the personal data persists.

6. Rectification, blocking, flagging and erasure must be notified to the data subject and to all those to whom the data were previously disclosed for processing. Notification may be omitted if this does not harm the legitimate interests of the data subject having regard to the purposes of the processing.
7. If the controller does not comply with the data subject's request for rectification, blocking or erasure, it shall, within 25 days of receipt of the request, communicate in writing or, with the data subject's consent, by



electronic means, the factual and legal grounds for refusing the request for rectification, blocking or erasure. In the event of refusal of a request for rectification, erasure or blocking, the controller shall inform the data subject of the possibility of judicial remedy and of recourse to the Authority. Contact details of the Authority:

**National Authority for Data Protection and Freedom of Information**

1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Postal address: 1530 Budapest, P.O. Box 5.

Phone: +36 -1-391-1400, E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

## **12. Objection to the processing of personal data**

1. The data subject may object to the processing of his or her personal data in accordance with Article 21 of the Info,
  - a. where the processing or transfer of personal data is necessary for the fulfilment of a legal obligation to which the controller is subject or for the purposes of the legitimate interests pursued by the controller, the recipient or a third party, except in cases of mandatory processing;
  - b. if the personal data are used or disclosed for direct marketing, public opinion polling or scientific research purposes; and
  - c. in other cases specified by law.
2. The controller shall examine the objection within the shortest possible time from the date of the request, but not later than 15 days, decide whether the objection is justified and inform the applicant in writing of its decision. If the data subject does not agree with the decision of the controller or if the controller fails to comply with the above deadline, the data subject may, within 30 days of the notification of the decision or the last day of the deadline, take the matter to court in the manner provided for in Article 22 of the Info Act.
3. If the controller establishes that the data subject's objection is justified, the controller shall terminate the processing, including further collection and further transfer, and block the data, and notify the objection and the action taken on the basis of the objection to all those to whom the personal data subject of the objection has previously disclosed the personal data subject and who are obliged to take measures to enforce the right to object. If the data controller does not receive the data necessary to exercise the data subject's right because of the data subject's objection, the data subject may, within 15 days of the notification as specified above, take legal action against the data controller in order to obtain access to the data, as provided for in Article 22 of the Info Act. The controller may also bring legal proceedings against the data subject.



4. If the data controller fails to give the notification referred to above, the data recipient may request clarification from the data controller of the circumstances surrounding the failure to transfer the data, which clarification the data controller shall provide within 8 days of the delivery of the data recipient's request. In the event of a request for clarification, the data subject may bring an action against the controller before a court within 15 days of the date on which the clarification was provided, but no later than the time limit for the provision of clarification. The controller may also bring legal proceedings against the data subject.
5. The controller may not delete the data of the data subject if the processing is required by law. However, the data may not be transferred to the data recipient if the controller has consented to the objection or if the court has ruled that the objection is justified.

### **13. Enforcement**

1. In the event of a breach of the data subject's rights, as well as in the cases specified in Article 21 of the Info Act, the data subject may take legal action against the controller. The court shall rule on the matter out of turn.
2. The court has jurisdiction to hear the case. The action may also be brought, at the option of the person concerned, before the court of the place where he or she is domiciled or resident.
3. A person who does not otherwise have legal capacity to sue can also be a party to the lawsuit. The Authority may intervene in the proceedings in order to ensure that the person concerned is successful.
4. If the court grants the application, the data controller shall be obliged to provide the information, rectify, block or erase the data, annul the decision taken by automated data processing, take into account the right of objection of the data subject, or release the data requested by the data recipient as defined in Article 21 of the Info Act.
5. If the court rejects the data subject's request in the cases specified in Article 21 of the Info Act, the controller is obliged to delete the data subject's personal data within 3 days of the judgment. The data controller shall also be obliged to delete the data if the data subject does not apply to the court within the time limit specified in Article 21(5) or (6) of the Info Act.
6. The court may order the publication of its judgment, with the publication of the data controller's identification data, if the interests of data protection and the rights of a larger number of data subjects protected by this Act so require.



#### **14. Damages and compensation**

1. If the data controller causes damage to another person by unlawful processing of the data subject's data or by breaching the requirements of data security, the data controller must compensate for the damage.
2. If the controller infringes the data subject's right to privacy by unlawfully processing his or her data or by breaching data security requirements, the data subject may claim damages from the controller.
3. The controller is liable to the data subject for any damage caused by the processor and the controller is also liable to pay the data subject the damages for any personal injury caused by the processor. The controller shall be exempted from liability for the damage caused and from the obligation to pay the damage fee if it proves that the damage or the infringement of the data subject's personality rights was caused by an unavoidable cause outside the scope of the processing.
4. No compensation shall be due and no damages shall be payable where the damage or injury to the person concerned has been caused by the intentional or grossly negligent conduct of the victim or by an infringement of a right relating to personality.

The date of entry into force of the GTC and any amendments thereto shall be the date of publication on the website of Kolt-Systems Kft.