PRIVACY NOTICE
regarding the processing of the data of contractual partners' contact personnel

Effective as of October 30, 2018

Virtual Solutions Korlátolt Felelősségű Társaság (seat: 1051 Budapest, Bajcsy-Zsilinszky út 12.; company reg. no. 01-09-199004; tax number: 25087721-2-41; hereafter referred to as: **Data controller** or **Company**) in accordance with with Regulation (EU) 2016/679 of the European Parliament and of the Council, the General Data Protection Regulation (hereafter referred to as **GDPR**) hereby informs its contract customer, buyer, dealer, reseller, distributor, supplier and (sub)contractor partners on the processing of the contact personnel data by the Data controller.

The present privacy notice is an inseparable annex to the contract between the Data controller and the contracted partner (including: contract customer, buyer, dealer, reseller, distributor, supplier and (sub)contractor partners).

The contracted partner shall hand over this notice to their contact persons and shall certify to Data controller the handing over of the notice.

1. What personal data do we process, for how long, for what purposes and by what authorization?

The legal bases for our data processing are the following:

a) GDPR Article 6 (1) f) where data processing is necessary for the purposes of the legitimate interests pursued by the Data controller or by a third party.

The processed data, the legal bases and the data processing purposes are as follows:

1.1. Customer/subcontractor contact personnel

A	B	C	D	E
Data category	**Data source**	**Purposes of data processing**	**Legal basis of data processing**	**Timeframe of data processing, deletion times**
Name	Customer/supplier, subcontractor	a) Concluding the contract b) Fulfilment of the contract c) Law enforcement d) Identification e) Communication	GDPR article 6 par. (1) f) point: legitimate interest of the Data controller and its customer/supplier, subcontractor	If the data are in the contract: 8 years from termination of the contract (in line with articles 168-169 of the Act Nr. C of 2000 on the Accounting („**Accounting Act**") for complying with the accounting obligation of the Data controller) If the data are not in the contract: 5 years from termination of the contract (in line with article 6:22. § par. (1) of Act Nr. V of 2013 on the Civil Code („**Civil Code**") for the enforcement of legal claims of the Data controller or defence against such legal claims)

E-mail address	Customer/supplier, subcontractor	a) Concluding the contract b) Fulfilment of the contract c) Law enforcement d) Communication	GDPR article 6 par. (1) f) point: legitimate interest of the Data controller and its customer/supplier, subcontractor	If the data are in the contract: 8 years from termination of the contract (in line with articles 168-169 of the Accounting Act for complying with the accounting obligation of the Data controller) If the data are not in the contract: 5 years from termination of the contract (in line with article 6:22. § par. (1) of the Civil Code for the enforcement of legal claims of the Data controller or defence against such legal claims)
Name and address of the company	Customer/supplier, subcontractor	a) Concluding the contract b) Fulfilment of the contract c) Law enforcement d) Identification e) Communication	GDPR article 6 par. (1) f) point: legitimate interest of the Data controller and its customer/supplier, subcontractor	If the data are in the contract: 8 years from termination of the contract (in line with articles 168-169 of the Accounting Act for complying with the accounting obligation of the Data controller) If the data are not in the contract: 5 years from termination of the contract (in line with article 6:22. § par. (1) of the Civil Code for the enforcement of legal claims of the Data controller or defence against such legal claims)
Phone number	Customer/supplier, subcontractor	a) Concluding the contract b) Fulfilment of the contract c) Law enforcement d) Communication	GDPR article 6 par. (1) f) point: legitimate interest of the Data controller and its customer/supplier, subcontractor	If the data are in the contract: 8 years from termination of the contract (in line with articles 168-169 of the Accounting Act for complying with the accounting obligation of the Data controller) If the data are not in the contract: 5 years from termination of the contract (in line with article 6:22. § par. (1) of the Civil Code for the enforcement of legal claims of the Data controller or defence against such legal claims)
Department, job title, position	Customer/supplier, subcontractor	a) Concluding the contract b) Fulfilment of the contract c) Law enforcement	GDPR article 6 par. (1) f) point: legitimate interest of the	If the data are in the contract: 8 years from termination of the contract (in line with articles 168-169 of the Accounting Act for

		d) Identification e) Communication	Data controller and its customer/supplier, subcontractor	complying with the accounting obligation of the Data controller) If the data are not in the contract: 5 years from termination of the contract (in line with article 6:22. § par. (1) of the Civil Code for the enforcement of legal claims of the Data controller or defence against such legal claims)

1.2. Potential customer (requesting bid) contact personnel

A	B	C	D	E
Data category	**Data source**	**Purposes of data processing**	**Legal basis of data processing**	**Timeframe of data processing, deletion times**
Name	Potential customer	a) Sending bid b) Identification c) Communication	GDPR article 6 par. (1) f) point: legitimate interest of the Data controller and potential customer	If the bid is not accepted: 1 year from the date of the offer If the bid is accepted: as specified regarding the processing of customer contact personnel data
E-mail address	Potential customer	a) Sending bid b) Communication	GDPR article 6 par. (1) f) point: legitimate interest of the Data controller and potential customer	If the bid is not accepted: 1 year from the date of the offer If the bid is accepted: as specified regarding the processing of customer contact personnel data
Name and address of the company	Potential customer	a) Sending bid b) Identification c) Communication	GDPR article 6 par. (1) f) point: legitimate interest of the Data controller and potential customer	If the bid is not accepted: 1 year from the date of the offer If the bid is accepted: as specified regarding the processing of customer contact personnel data
Phone number	Potential customer	a) Sending bid b) Communication	GDPR article 6 par. (1) f) point: legitimate interest of the Data controller and potential customer	If the bid is not accepted: 1 year from the date of the offer If the bid is accepted: as specified regarding the processing of customer contact personnel data
Department, job title, position	Potential customer	a) Sending bid b) Communication	GDPR article 6 par. (1) f) point:	If the bid is not accepted: 1 year from the date of the offer

			legitimate interest of the Data controller and potential customer	If the bid is accepted: as specified regarding the processing of customer contact personnel data

1.3. Legitimate interest

a) **Law enforcement:** in this case, the purpose of data processing is law enforcement. These data are processed by the Data controller to be used as evidence in the event of a possible legal dispute with the partner. This right of the Data controller shall be practiced in line with the relevant statute of limitations, therefore the data processing is necessary for safeguarding the Data controller's rights and legitimate interests. The purpose of data processing may not be reached by any other measure.

b) **Communication concerning the conclusion and the fulfilment of the contract, identification:** it is the business interest of the Data controller and its contracted partner to communicate with each other concerning the contract. The purpose of data processing may not be reached by any other measure, the communication may not be conducted without contact data.

c) **Sending bid:** it is the legitimate interest of the Data and the potential customer controller to send bids, to expand its business and contract relations and to improve its economic capacities.

The data subject has the right to object concerning the data processing based on legitimate interest, in which case the Data controller shall further not process the data, unless it 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.

2. Who manages your personal data, and who has access to them?

2.1. The data controller

The controller of the personal data specified under point 1 hereto and its contacts and company data are as follows:

Virtual Solutions Kft.
Company reg. no.: 01-09-199004
Tax no.: 25087721-2-41
Seat: 1051 Budapest, Bajcsy-Zsilinszky út 12.
Postal address: 1051 Budapest, Bajcsy-Zsilinszky út 12.
E-mail address: info@cloudstorm.io

On behalf of the Data controller, the data are accessible by the employees of the Data controller whose access is essential to the performance of their duties. Access authorizations are specified in a strict internal code.

2.2. Data processors

For the processing of the personal data of representative and contact persons, we engage the following companies as data processors, which conduct the following processing operations on behalf of the Data controller:

Name and contacts of data processor	Purpose of data processing	Data subjects affected by data processing	Data processed
The Rocket Science Group, LLC Mailing address: 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 Amerikai Egyesült Államok	Providing Mailchimp, online e-newsletter sending system	Customers' contact persons	Name, e-mail address
Atlassian, Inc. (Trello, Inc.) Seat: 1098 Harrison Street San Francisco, California 94103, USA	Providing Trello Services, a task management application	Contact persons of the customers/suppliers, subcontractors	Name, e-mail address, phone number, position, company name
Slack Technologies, Inc. Seat: 500 Howard Street San Francisco, California 94105	Providing Slack Services, a collaboration and communication hub	Contact persons of the customers/suppliers, subcontractors	Name, e-mail address, phone number, position, company name, personal data in the message
Zapier, Inc. Seat: 548 Market St #62411 San Francisco, California 94104, USA	Providing IT services, connection of communication applications	Contact persons of the customers/suppliers, subcontractors	Name, e-mail address, phone number, position, company name, personal data in the message
GitHub, Inc. Seat: 88 Colin P Kelly Jr Street San Francisco, California 94107, USA	Providing IT services, source-code escrow services	Customers' contact persons	Name, e-mail address, company name
Amazon.com, Inc. (Amazon Web Services, Inc.) Seat: 2021 Seventh Ave Seattle, Washington 98121,	As data processor of Virtual Solutions Kft as data controller: Providing cloud services	Contact persons of customers/potential customers/suppliers, subcontractors	Contact persons of customers/suppliers, subcontractors: name, e-mail address, phone number, position, company name

USA	Host provider (website hosting)		Contact persons of potential customers: name, e-mail address, department/job title/position, company name, phone number
Intercom, Inc. Intercom R&D Unlimited Company Seat: 55 2nd Street, 4th Floor San Francisco, California 94105, USA	Providing customer messaging platform	Customers' contact persons	Name, e-mail address, department, company name, any personal data in the message
Microsoft Corporation Seat: One Microsoft Way Redmond, Washington 98052, USA	Microsoft 365 Services (cloud) Microsoft Azure services (cloud)	Contact persons of customers/potential customers/suppliers, subcontractors	Contact persons of customers/suppliers, subcontractors: name, e-mail address, phone number, position, company name Contact persons of potential customers: name, e-mail address, department/job title/position, company name, phone number
GOOGLE LLC Seat: 1600 Amphitheatre Pkwy Mountain View, California 94043, USA	Providing Google Drive (Cloud), Google Analytics for Display Advertising, Google Ad Manager Audience Extension, Google Ads Remarketing, e-mail services, Tag manager services	Contact persons of customers/potential customers/suppliers, subcontractors	Contact persons of customers/suppliers, subcontractors: name, e-mail address, phone number, position, company name Contact persons of potential customers: name, e-mail address, department/job title/position, company name, phone number

Information concerning data transfer to third countries:

From the above data processors, the entities seated in the USA (The Rocket Science Group, LLC, Atlassian, Inc. (Trello, Inc.), Slack Technologies, Inc., Zapier, Inc., GitHub, Inc., Amazon.com, Inc. (Amazon Web Services, Inc.), Microsoft Corporation, Google LLC) are on the U.S. – EU Privacy Shield List set up based on the adequacy decision laid down in Article 45 of the GDPR and by the regulation 2016/1260 of the European Commission, thus data transfer to these companies shall not be considered as data transfer to third countries, outside of the EU, and the explicit consent of the data subjects is not required, furthermore transferring data to these companies is allowed under Article 45 of the GDPR. These companies undertook to comply with the GDPR.

2.3. Who is the data protection officer of the Data controller and what are its contact details?

Dr. Levente Lojek
Bovard Adatvédelmi and Szolgáltató Kft.
Seat: 1123 Budapest, Greguss utca 12. fszt. 5.
Registration number: 01-09-303569
Tax number: 26131562-2-43
E-mail: info@bovard.hu

3. What rights do contact persons have regarding the processing of their data, and how can they exercise them?

3.1. Data protection rights and remedies

The detailed rights and remedies of the individuals are set forth in the applicable provisions of the GDPR (especially in articles 15, 16, 17, 18, 19, 21, 22, 77, 78, 79, 80, and 82 of the GDPR). The summary set out below describes the most important provisions and the Company provides information for the individuals in accordance with the above articles about their rights and remedies related to the processing of personal data.

The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the individual, information may also be provided orally, provided that the identity of the individual is proven by other means.

The Company will respond without unreasonable delay and by no means later than within one month of receipt to the request of an individual whereby such person exercises his/her rights about the measures taken upon such request (see articles 15-22 of the GDPR). This period may be, if needed, extended by further two months in the light of the complexity of the request and the number of requests to be processed. The Company notifies the individual about the extension also indicating its grounds within one months of the receipt of the request. Where the request has been submitted by electronic means, the response should likewise be sent electronically unless the individual otherwise requests.

In case the Company does not take any measure upon the request, it shall so notify the individual without delay but by no means later than in one month stating why no measures are taken and about the opportunity of the individual to lodge a complaint with the data protection authority and to file an action with the courts for remedy.

3.2. The individual's right of access

(1) The individual has the right to obtain confirmation from the Company whether or not personal data concerning him/her are being processed. Where the case is such, then he/she is entitled to have access to the personal data concerned and to the following information:

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed including especially recipients in third countries and/or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the right of the individual to request from the Company rectification or erasure of personal data or restriction of processing of personal data concerning the individual or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the individual, any available information as to their source.

(2) Where personal data are forwarded to a third country, the individual is entitled to obtain information concerning the adequate guarantees of the data transfer.

(3) The Company provides a copy of the personal data undergoing processing to the individual. The Company may charge a reasonable fee based on administrative costs for requested further copies. Where the individual submitted his/her request in electronic form, the response will be provided to him/her by widely used electronic means unless otherwise requested by the individual.

3.3. Right to rectification

The individual has the right to request that the Company rectify inaccurate personal data which concern him/her without undue delay. In addition, the individual is also entitled to have incomplete personal data completed e.g. by a supplementary statement or otherwise.

3.4. Right to erasure ('right to be forgotten')

(1) The individual has the right that when he/she so requests, the Company erase the personal data concerning him/her without 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 by the Company;
(b) the individual withdraws consent on which the processing is based, and is no other legal ground subsists for the processing;
(c) the individual 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 Company is subject;
(f) the collection of the personal data occurred in connection with offering services regarding the information society.

(2) In case the Company has made the personal data public and then it becomes obliged to delete it as aforesaid, then it will, taking into account the available technology and the costs of implementation, take reasonable steps including technical steps in order to inform processors who carry out processing that the individual has initiated that the links leading to the personal data concerned or the copies or reproductions of these be deleted.

(3) Paragraphs (1) and (2) shall not apply to the extent that processing is necessary, among other things, for:

a) exercising the right of freedom of expression and information;
b) compliance with a legal obligation which requires processing by Union or Member State law to which the Company is subject;

c) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
d) the establishment, exercise or defence of legal claims.

3.5. Right to restriction of processing

(1) The individual has the right to obtain a restriction of processing from the Company where one of the following applies:

a) the accuracy of the data is contested by the individual, for a period enabling the Company to verify the accuracy of the personal data;
b) the processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of their use instead;
c) the Company no longer needs the personal data for the purposes of the processing, but the individual requires them for the establishment, exercise or defence of legal claims;
d) the individual has objected to processing based on the legitimate interest of the Company pending the verification whether the legitimate grounds of the Company override those of the individual.

(2) Where processing has been restricted under paragraph (1), such personal data shall, with the exception of storage, only be processed with consent of the individual 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) The Company informs the individual whose request has served as grounds for the restriction based on the aforesaid, before the restriction of processing is lifted.

3.6. Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Company will communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Company informs the individual about those recipients if he/she so requests.

3.7. Right to object

The individual has the right to object, on grounds relating to his/her particular situation, at any time to processing of personal data concerning him/her for the purposes of legitimate interests. The Company will no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual or for the establishment, exercise or defence of legal claims.

3.8. Right to lodge a complaint with a supervisory authority

The individual has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his/her habitual residence, place of work or place of the alleged infringement if he/she considers that the processing of personal data relating to him/her infringes the GDPR. In Hungary, the competent supervisory authority is the Hungarian Authority for Data Protection and Freedom of Information (http://naih.hu/; 1530 Budapest, Pf.: 5; telephone: +36-1-391-1400; fax: +36-1-391-1410; e-mail: ugyfelszolgalat@naih.hu).

3.9. Right to an effective judicial remedy against a supervisory authority

(1) The individual has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning him/her.

(2) The individual has the right to an effective judicial remedy where the supervisory authority which is competent does not handle a complaint or does not inform him/her within three months on the progress or outcome of the complaint lodged.

(3) Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

3.10. Right to an effective judicial remedy against the Company or the processor

(1) The individual, without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, has the right to an effective judicial remedy where he/she considers that his/her rights under the GDPR have been infringed as a result of the processing of his/her personal data in non-compliance with the GDPR.

(2) Proceedings against the Company or a processor shall be brought before the courts of the Member State where the Company or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the individual has habitual residence. In Hungary, in these kinds of proceedings the general court has jurisdiction. The proceedings can be brought - according to the choice of the individual concerned - before the general court where one has its habitual residence or place of stay. Information on the competent courts is available at www.birosag.hu.

4. How do we ensure the safety of their data?

In order to ensure data, IT and information security, we accepted and use System Development Life Cycle (SDLC) Policy, SDLC Standard, System Development and Operation (SDO) Policy and Information Security Policy. Our employees, subcontractors and suppliers are obliged to act and work according to those aforementioned policies.

Data security measures in software development

- All software developed according to the SDLC standards.
- Software development is based on preliminary analysis or feasibility studies, risk identification and mitigation, system analysis.
- All software development process include quality assurance and acceptance testing.
- All software developed by us are adequately documented and tested before it is used.
- All development work exhibit a separation between production, development and test environments. Development, QA and test staff is not entitled to have access to production systems unless absolutely required by their respective job duties.
- Documentation is kept and updated during all phases of development, security considerations are noted and addressed through all phases of development.
- We use the industry best practices during the software development.

Information security measures concerning staff:

- We train our employees and our external developers on a regular basis concerning data protection and data/information and IT security. Each new employee/external developer is obliged to take part in the security training.

- End user authentication use unique user identifiers, strong passwords or two factor authentication.
- Passwords shall be changed on a regular basis, according to the Information Security Policy.

Information security in the maintenance of the software:

- Only the designated employees have access to the software or the personal data processed by the software or stored in the SaaS services by the Customers.
- Any planned changes to the system are scheduled, communicated and documented.
- Continuous security penetration testing is concluded on the system and the software throughout its life-cycle at regularly scheduled intervals.
- Mandatory security testing is conducted when any major configuration or architecture change is made.
- We keep all deployed systems up-to-date with the latest security-related patches issued by the system vendors.

Security measures during the daily work:

- Remote access to personal workstations is allowed only with unique usernames and passwords and in encrypted channels to transfer traffic.
- All access to production system are limited according to our SDLC Policy.
- We use cloud-based systems for storing the system, software and personal data. Access to those cloud systems are restricted according to the SDLC and IT Security Policies.
- We protect our systems with appropriate firewalls.
- We use clean desk and clean whiteboard policy according to our Information Security Policy.

Security measures concerning Customer's data

- All customer's data are stored by us are adequately isolated from other Customer's data.
- Data storage containing Customer's data always is protected with automatic encrypted backups. Backup frequency is daily.
- We do not use offline media for storing data backups, instead the data are stored on durable cloud based storage services that provide comprehensive security and compliance capabilities and meet ISO 27001 certificate.
- We use multiple, geographically separated backups

Security measures in communication

- All data transfer are happen through secure channels using HTTPS or SSL or equivalent protocols.
- All administrative traffic, traffic going to or coming from external services go through secure channels using HTTPS or SSL or equivalent protocols.

5. What procedure do we follow upon an incident?

Pursuant to applicable law, we report incidents to the supervisory authority within 72 hours of having gained knowledge thereof, and we also keep records of them. In cases regulated by applicable law, we also inform subjects of the incidents, where necessary.

6. When and how do we amend this notice?

Should the scope of data, or the circumstances of data processing be subject to change, this notice shall be amended and sent out or otherwise provided to the data subjects as is required by GDPR. Please pay attention to the amendments of this notice, as they contain important information regarding the processing of your personal data.