PRIVACY POLICY

Last modified: March 18, 2021

This Privacy Policy (the "Policy") explains how GhostMonitor Inc. ("GhostMonitor", "Company," "we," or "us") collects, stores, uses, and discloses personal information from our users ("you", "user") in connection with the website located at www.recart.com and all its subdomains and subpages thereto (the "Website").

Please read and make sure you understand this Policy, our Data Protection Addendum attached to the present Policy as *Annex 1* (hereinafter: "Addendum"), which also serves as Standard Contractual Clauses in accordance with the GDPR defined below and which forms an inseparable part of the present Policy. the present Policy shall be construed in a manner of the provisions of the Addendum. If you do not agree with this Policy, the Addendum or our practices, you may not use our Website or our services (the "Services"). This Policy may change from time to time and is incorporated into our Website Terms of Use. Your continued use of our Website and Services constitutes your acceptance of those changes. We encourage you to review this Policy periodically.

The processing and collecting of personal data by GhostMonitor shall be in harmony with the directly applicable data protection laws in effect:

(i) In case of processing personal data of you either as a natural person or a legal entity's representative located in the European Union ("EU"), the regulation 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 Directive 95/46/EC ("GDPR"), furthermore the recommendations of the Article 29 Data Protection Working Party ("WP29") and of the European Data Protection Board ("EDPB") shall apply;

(ii) For the collection and processing of personal data of Brazilian individuals, Brazil's Law No. 13,709, of August 14, 2018 on the Brazilian General Data Protection Act (in Portuguese: Lei Geral de Proteção de Dados, "LGPD") shall apply;

(iii) Furthermore, in respect of Californian individuals GhostMonitor complies with the Senate Bill No. 1121 California Consumer Privacy Act of 2018 ("CCPA") shall apply;

Please note that the present Policy applies to the data processing relationship between GhostMonitor and you either as a natural person, or as a legal entity's representative. In relation to users as natural person located within the European Union ("EU") member countries, according to the provisions of the GDPR, GhostMonitor shall be deemed as data controller.

By using the Services of GhostMonitor – as described under section 2.3 of the present Policy – you as our user shall be deemed as a data controller and GhostMonitor shall be considered as a data processor. The

rights and obligations regarding to that relationship between you as data controller and GhostMonitor as data processor is governed by the Addendum attached to the present Policy as *Annex1*.

GhostMonitor may from time to time handle personal data collected from individuals located within the European Union ("EU") member countries. Consistent with GDPR GhostMonitor grants the enhanced data protection for the individuals located within the EU. Our adherence to the GDPR regarding the personal data collected from individuals located within the EU is detailed in this Policy.

Furthermore, GhostMonitor complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, onward transfer and retention of personal data transferred from EU member countries and Switzerland to the United States, respectively. GhostMonitor has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield principles ("Privacy Shield Principles") of:

- Notice
- Choice
- Accountability of onward transfer
- Security
- Data integrity and purpose limitation
- Access
- Recourse, enforcement and liability

Our adherence to each of these principles is detailed in this Policy. If there is any conflict between the terms of the Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. If you want to learn more about the Privacy Shield program or view GhostMonitor's certification, please visit https://www.privacyshield.gov.

GhostMonitor is under the jurisdiction as well as the investigatory and enforcement powers of the US Federal Trade Commission for purposes of the EU-US Privacy Shield framework and the Swiss-US Privacy Shield Framework.

1. What does this Privacy Policy cover?

This Policy covers GhostMonitor's treatment of information that GhostMonitor gathers when you are accessing GhostMonitor's Website as a user and when you use GhostMonitor Services. Also, this Policy covers GhostMonitor's treatment of your information that GhostMonitor shares with GhostMonitor's business partners. This Policy does not apply to the practices of third parties that GhostMonitor does not own or control (such as third-party websites that you may access from the Website), or to individuals that GhostMonitor does not employ or manage.

2. What information does GhostMonitor collect?

The information we gather from users enables GhostMonitor to personalize and improve our services and to allow our users to set up accounts on the Website. While we are providing our Services, we receive certain data from third parties (e.g. Facebook) about the customers of our users. We collect the following types of information from our users and their customers:

2.1 Information You Provide to Us:

We receive and store any information you enter on our Website or provide to us in any other way including registering an account on our affiliate site (https://www.recart.leaddyno.com). The types of information collected include, without limitation, your full name, email address, mailing address, phone number, password, contact information and content consumed on the Website, including, but not limited to content uploaded and shared. Some of this information is not mandatory but is necessary to use all of our functions.

In addition, we collect the following financial data: account holder name, bank name, account number, currency of account. For taxation reasons, we need to collect Tax ID (US: tin: SSIN/EIN), citizenship, country of residence. In some cases, we'll need to ask for a government ID, Green Card, or other proof of address or proof of residency status as regulated by taxation law.

2.2 Information Collected Automatically:

We receive and store certain types of information whenever you interact with our Website or Services. GhostMonitor automatically receives and records information on our server logs from your browser including your IP address, unique device identifier, browser characteristics, domain and other system settings, search queries, device characteristics, operating system type, language preferences, referring URLs, actions taken on our Website, page requested, content consumed (e.g., viewed, uploaded, and shared), dates and times of Website visits, and other information associated with other files stored on your device.

2.3 Information we receive from third parties:

By providing our Services we receive and collect certain personal data on the customers of our users that is provided to us by third parties (e.g. Facebook or our affiliate). If the provisions of the GDPR shall apply, in that relationship regarding to the personal data of your customers you shall be deemed as data controller, and therefore you are responsible to comply with the provisions of the GDPR. Please note, that in such case the data processing relationship between the data controller and the data processor shall be governed by a written contract, and such written contract shall satisfy the requirements of Article 28 of the GDPR. In order to facilitate your compliance with the provisions of the GDPR, GhostMonitor provides you a written contract on data processing, therefore, the data processing relationship between you, as a data controller and GhostMonitor, as a data processor shall be governed by the Addendum attached to the present Policy as *Annex1*, which shall form an integral part of the present Policy.

3. What About Cookies?

The Company collects mainly anonymous data from the Website, such as searches. The anonymized data can include user session data such as IP address, web browser type, the time spent on the page by the user, and user-clicked buttons. The Company processes anonymous data in order to improve the page, to bring it to perfection. During this procedure GhostMonitor can incorporate "cookies", which collect the visitor's first level domain name, the date and the exact time of access. The "cookie" alone can't be used to reveal the identity of the visitor. The "cookie" is a file, which is sent to the browser of the visitor and stored on

the hard drive of visitor. Cookies don't damage the computer of the visitor. The browser can be set to indicate when a cookie is received, so the visitor can decide to accept the so-called cookie or not. The Company does not use cookies to collect or manage any information that would allow the identification of the user. Please see our cookie policy by visiting the following **link** in order to find out how our cookies work.

4. How Does GhostMonitor Use My Information?

We may use your information, including your personal information - based on diverse purposes as well as the legal basis of the processing - as follows:

4.1. We process the following personal data for the purpose and on the legal basis of the **performance of the contract**, **product and service fulfillment**:

- Full name
- Email address
- Mailing address
- Phone number
- Financial data: account holder name, bank name, account number, currency of account

The information you provide is used for purposes such as responding to your requests for certain products and services, customizing the content you see, communicating with you about specials, sales offers, and new features, and responding to problems with our services. It is also used to fulfill and manage payments or requests for information, or to otherwise serve you, provide any requested services and administer sweepstakes and contests.

4.2. We process the following personal information based on your consent (as the legal basis of this processing) for **marketing purposes**, **to deliver coupons, mobile coupons, newsletters, receipt messages, e-mails, and mobile messages**. We also send marketing communications and other information regarding services and promotions based on your consent and administer promotions:

- Full name
- Email address
- Mailing address
- Phone number (optional)

You shall always have the right to withdraw your consent at any time.

4.3. We process personal data for the purpose and on the legal basis of **compliance with legal obligations** to prevent fraudulent transactions, monitor against theft and otherwise protect our customers and our business. We also process personal data for the purpose and on the legal basis of **legal compliance** and to assist law enforcement and respond to subpoenas.

This means that in some cases the data processing is stipulated by the applicable laws and we have an obligation to process and keep this data for the required time. This includes employment data, billing data, data which is necessary to assist law enforcement etc.

4.4. We process the following personal data for the purpose and on the legal basis of the **legitimate interests of the Company, to improve the effectiveness** of the Website, our Services, and marketing efforts, to conduct research and analysis, including focus groups and surveys and to perform other business activities as needed, or as described elsewhere in this Policy:

- IP address
- browser information
- password
- contact information
- content consumed on the Website
- unique device identifier
- browser characteristics
- domain and other system settings
- search queries
- device characteristics
- operating system type
- language preferences
- referring URLs
- actions taken on our Website
- page requested
- content consumed (e.g., viewed, uploaded, and shared)
- dates and times of Website visits
- other information associated with other files stored on your device

Where it is feasible we anonymize personal data or use non-identifiable statistical data. We do not collect personal data in advance and store it for potential future purposes unless required or permitted by the applicable laws.

For collecting anonymously the above-mentioned data and making statistics and analysis we may use the following software and programs:

Name	**Registered seat**	**Country**
Google Analytics and Google AdWords (Google LLC.)	1600 Amphitheatre Parkway Mountain View, CA 94043	United States of America
Intercom, Inc.	55 2nd Street, 4th Floor, San Francisco, California 94105	United States of America
Facebook pixel (Facebook Inc.)	1601 Willow Road Menlo Park, CA 94025	United States of America

4.5. **Cookies**: GhostMonitor may use automatically collected information and cookies information to: (a) remember your information so that you will not have to re-enter it during your visit or the next time you visit the Website; (b) provide custom, personalized advertisements, content, and information; (c) monitor the effectiveness of our marketing campaigns; and (d) monitor aggregate usage metrics such as total number of visitors and pages viewed.

4.6. **Data integrity and purpose limitation**: GhostMonitor will only collect and retain personal data which is relevant to the purposes for which the data is collected, and we will not use it in a way that is incompatible with such purposes unless such use has been subsequently authorized by you. We will take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current. We may occasionally contact you to determine that your data is still accurate and current. To secure your personal information processed we save your personal information to backup archives in every 24 hours. The data stored in our backup archives will be deleted in every half a year.

5. How Long We Retain Your Personal Data?

We will retain your personal data for so long as it is needed to fulfill the purposes outlined in this Policy or until you withdraw your consent, unless a longer retention period is required or permitted by law (such as tax, accounting or other legal requirements). When we have no longer or no legal basis to process your personal information, we will either delete or anonymize it, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

6. Will GhostMonitor share any of the information it receives?

Information about our users is an integral part of our business, and we may share such information with our affiliated entities. Except as expressly described below, we neither rent nor sell your information to other people or nonaffiliated companies unless we have your permission.

6.1 Third Party Service Providers:

We may share certain personal information with third party vendors who supply software applications, web hosting and other technologies for the Website and the Services. We will only provide these third parties with access to information that is reasonably necessary to perform their work or comply with the law. Those third parties will never use such information for any other purpose except to provide services in connection with the Website and the Services. We may also share aggregated or de-identified information, which cannot reasonably be used to identify you. We may also request data process service for processing the personal data. During the service of data process, the data processor shall abide under the present Policy, relevant legislations in force, furthermore the provisions of the existing contracts of the GhostMonitor.

6.2 List of Third Party Service Providers:

Name of Provider	Registered Seat	Country	Activity (data processing service)
Amazon Web Services, Inc. (Amazon Web Services)	410 Terry Avenue North Seattle, WA 98109	United States of America	Server providing services
MongoDB, Inc.	1633 Broadway, 38th Floor, New York, NY 10019	United States of America	Document database

Intercom, Inc.	55 2nd Street, 4th Floor San Francisco, California 94105	United States of America	Customer support services
HotJar Ltd.	Level 2, St Julian's Business Centre, 3, Elia Zammit Street, St Julian's STJ 1000	Malta	Behavior analytics and user feedback service, combines analysis and feedback tools
Google LLC. (Google Analytics)	1600 Amphitheatre Parkway Mountain View, CA 94043	United States of America	Web analytics service that tracks and reports traffic on the Website
Segment.io, Inc.	100 California St Suite 700, San Francisco, California 94111	United States of America	Helps developers manage all the analytics data their apps and services generate
Hull, Inc. (Hull.io)	3423 Piedmont Rd NE Atlanta, Georgia 30305	United States of America	Centralizes data from online and offline sources
LogRocket, Inc.	101 Main Street, Cambridge, Massachusetts 02142	United States of America	Helps developers to fix bugs, errors and other issues that may occur during the operation of the Services.
HubSpot, Inc.	25 1st Street Cambridge, MA 02141	United States of America	CRM platform
Vitally, Inc. (vitally.io)	247 Water St, Brooklyn, NY 11201	United States of America	Customer support services

6.3 Transfer of Personal Data collected from individuals located within the EU:

Our service providers, Amazon Web Services, Inc., MongoDB, Inc., Intercom, Inc., Google LLC, Segment.io, Inc.Hull, Inc. LogRocket, Inc. and HubSpot, Inc. have their registered seat in the United States and they comply with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework, therefore transfer of your personal data to the aforementioned service providers was deemed safe until July 16, 2020. Please note that according to the judgement no. C-311/18 of the Court of Justice of the European Union, these companies are no longer considered to provide appropriate safeguards for the personal data of European citizens. For more information, you can read the judgement **here**.

If we transfer personal data collected from individuals located within the EU to a third-party acting as a data processor, and such third-party agent processes your personal information in a manner inconsistent with the GDPR or – having a registered seat in the United States of America – with the Privacy Shield Principles, we may be responsible under the rules of the GDPR and / or under Privacy Shield Principles.

We only transfer personal data collected from individuals located within the EU only with the consent of the individuals to a third-party having a registered seat outside the EU or the United States of America acting as a data processor without the appropriate safeguards set out in the

GDPR, or when it is necessary for the performance of the contract. GhostMonitor will make every effort to ensure that the personal data transferred is safe and secure and that the personal data is processed in a manner consistent with the GDPR.

6.4 GhostMonitor may release your information:

(a) in response to subpoenas, court orders or legal process, to the extent permitted and as restricted by law;

(b) when disclosure is required to maintain the security and integrity of the Website, or to protect any user's security or the security of other persons, consistent with applicable laws;

(c) when disclosure is directed or consented to by the user who has input the personal information; or

(d) in the event that we go through a business transition, such as a merger, divestiture, acquisition, liquidation or sale of all or a portion of its assets, your information will, in most instances, be part of the assets transferred.

6.5 Opt-In for Promotions:

We do not share personally identifiable information with other third-party organizations for their marketing or promotional use without your consent or except as part of a specific program or feature for which you will have the ability to opt-in.

6.6 With Your Consent:

Except as set forth above, you will be notified when your information may be shared with third parties and will have the option of preventing the sharing of this information.

6.7 Data retention and aggregated data processing

Please note that we may retain certain personal information after your account has been terminated. We reserve the right to use your information in any aggregated data collection after you have terminated your account, however we will ensure that the use of such information will not identify you personally.

6.8 Accountability for onward transfer:

GhostMonitor will not transfer personal data originating in the EU or Switzerland to third parties unless such third parties have entered into an agreement in writing with us requiring them to provide at least the same level of privacy protection to your personal data as required by the GDPR and / or Privacy Shield Principles. We acknowledge our liability for such data transfers to third parties.

By registration on the Website you give your express consent to the transfer of the personal data as detailed above.

7. Is information about me secure?

We take commercially reasonable measures to protect all collected information from loss, theft, misuse and unauthorized access, disclosure, alteration and destruction. Please understand that you can help keep your

information secure by choosing and protecting your password appropriately, not sharing your password and preventing others from using your computer. Please understand that no security system is perfect and, as such, we cannot guarantee the security of the Website, or that your information won't be intercepted while being transmitted to us. If we learn of a security systems breach, then we may either post a notice, or attempt to notify you by email and will take reasonable steps to remedy the breach.

8. Children's Privacy

Our Website is not directed to children under 16 and we do not knowingly collect personal information from children under 16. If we learn that we have collected personal information of a child under 16 we will take steps to delete such information from our files as soon as possible. If you are aware of anyone under 16 using the Website, please contact us at gdpr@recart.com.

9. Links to Third Party Sites and Services

This Website may contain links to third party websites operated by individuals or companies unrelated to us. Please be aware that we are not responsible for the privacy practices of such third party websites and services. We provide links to these websites for your convenience only and you access them at your own risk. We recommend that you review the privacy policies and terms of use posted on and applicable to such third party websites prior to utilizing them.

10. Your Privacy Rights

10.1 Access and Retention:

If you have a Website account, you can log in to view and update your account information. You have the right to obtain confirmation of whether or not we are processing personal data relating to you, have communicated to you such data so that you could verify its accuracy and the lawfulness of the processing and have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Privacy Shield Principles.

We encourage you to contact us at gdpr@recart.com with your questions or concerns, or to request edits to your personal information, or to have it removed from our database. Requests to access, change or remove your personal data will be handled within 30 days.

10.2 Additional Rights for EU Territory:

If you are from the territory of the EU, you may have the right to exercise additional rights available to you under applicable laws, including:

(a) **Right of Erasure**: In certain circumstances, you may have a broader right to erasure of personal information that we hold about you – for example, if it is no longer necessary in relation to the purposes for which it was originally collected. Please note, however, that we may need to retain certain information for record keeping purposes, to complete transactions or to comply with our legal obligations.

(b) **Right to Object to Processing**: You may have the right to request GhostMonitor to stop processing your personal information and/or to stop sending you marketing communications.

(c) **Right to Restrict Processing**: You may have the right to request that we restrict processing of your personal information in certain circumstances (for example, where you believe that the personal information, we hold about you is inaccurate or unlawfully held).

(d) **Right to Data Portability**: In certain circumstances, you may have the right to be provided with your personal information in a structured, machine readable and commonly used format and to request that we transfer the personal information to another data controller without hindrance.

If you would like to exercise such rights, please contact us at gdpr@recart.com. We will consider your request in accordance with applicable laws. To protect your privacy and security, we may take steps to verify your identity before complying with the request.

For any complaints that we can't resolve directly, please contact our European representative, **Recart Technologies Limited Liability Company** (registered seat: 1061 Budapest, Király utca 26., Hungary; company registration number: 01-09-281497; e-mail address: gdpr@recart.com).

You also have the right to complain to any EU Data Protection Authority about our collection and use of your personal data. For more information, please contact your local EU Data Protection Authority.

10.3 Additional Rights for Brazilian individuals

If you are a Brazilian individual, you have the following rights in addition to the rights described in section 9.1 of this Policy:

(a) **Right of erasure:** If you would exercise this right, we will respond to you immediately, or if that is not possible, we will send a reply to you to indicate the reasons of fact or law that prevents the immediate adoption of the measure. If we are not the data processors of the data you requested the erasure of – whenever possible – we will indicate who the processing agent is.

(b) **Right to be informed:** You have the right to obtain information about what types of processing do we carry out on your personal information.

(c) **Right of access:** If you request the providing of your personal data processed by us, we will grant you access to such data in 15 days of your request, if the data requested is more than the simplified request version.

(d) **Nondiscrimination:** We do not process your data for unlawful or abusive discriminatory purposes. In certain circumstances, you have the right to request a review of our data processing and the supervisory authority (the Brazilian National Authority for Protection of Data ("ANPD")) may carry out an audit to verify discriminatory aspects.

(e) **Data portability:** Your data might be transferred to another service or product supplier in accordance with the regulations of the ANPD and as subjects to commercial and industrial secrets.

GhostMonitor appointed Dávid Tóth (address: 1061 Budapest, Király utca 26.; e-mail address: gdpr@recart.com) as data protection officer ("**DPO**") in accordance with item II of Article 23 of the LGPD.

If you would like to exercise the rights included in the present section of the Policy, please contact our DPO or GhostMonitor at gdpr@recart.com. We will consider your request in accordance with

applicable laws. To protect your privacy and security, we may take steps to verify your identity before complying with the request.

You also have the right to complain to the ANPD about our collection and use of your personal data. For more information, please contact the ANPD.

11. Recourse, Enforcement and Liability

11.1 GhostMonitor is committed to protecting your personal data as set forth in this Policy. If you think we are not in compliance with our Policy, or if you have any question or if you wish to take any other action concerning this Policy, contact us at gdpr@recart.com. You can also contact us at our contact office at 251 Little Falls Drive, City of Wilmington, County of New Castle, Delaware 19808, USA. We will investigate your complaint, take the appropriate action and report back to you within 30 days. In addition, if you are from the territory of the EU, you also have the right to complain to the EU Data Protection Authority about our collection and use of your personal data. For more information, please contact your local EU Data Protection Authority.

11.2 If your personal data in question was transferred from the EU or Switzerland to the United States and you are not satisfied with our response, we have further committed to refer unresolved Privacy Shield complaints to the dispute resolution procedures of the EU Data Protection Authorities. GhostMonitor will cooperate with the appropriate EU Data Protection Authorities during investigation and resolution of complaints concerning personal data that is transferred from the EU to the United States brought under Privacy Shield. For complaints involving personal data transferred from Switzerland, we commit to cooperate with the Swiss Federal Data Protection and Information Commissioner ("FDPIC") and comply with the advice given by the FDPIC. Complaints regarding processing of personal data pertaining to data subjects located in the EU and Switzerland may be reported by the individual to the relevant Data Protection Authority.

11.3 The recourse mechanisms detailed in 11.1 and 11.2 are independent recourse mechanisms and they are available at no cost to you. Damages may be awarded in the accordance with the applicable law.

11.4 You may be able to invoke binding arbitration under certain conditions with the arbitrational mechanism of the American Arbitration Association, if you are not satisfied with the above recourse mechanism. The arbitration is available to you to determine, for residual claims, whether GhostMonitor has violated its obligations under the Principles as to you, and whether any such violation remains fully or partially unremedied.

11.5 Your decision to invoke the binding arbitration option is entirely voluntary. The arbitral decisions will be binding on all parties to the arbitration.

12. Modifications to this Policy

We will modify this Policy if our privacy practices change. We will notify you of such changes by posting the modified version on our Website and indicating the date it was last modified, and, if the changes are significant, we will provide a more prominent notice (including by email in certain instances). The date this

Policy was last modified is at the top of this page. Please periodically review this Policy so that you are familiar with the current Policy and aware of any changes.

13. For California Users

If you are a user in California, the Company's Privacy Notice for California Consumers applies to you, which is available **here**.

We will not share any personal data with third parties for their direct marketing purposes to the extent prohibited by California Consumer Privacy Act of 2018 ("CCPA"). If our practices change, we will do so in accordance with applicable laws and will notify you in advance.

14. Questions

If you have any questions concerning this Policy or the Services, please contact us at gdpr@recart.com. You can also contact us at our contact office at 251 Little Falls Drive, City of Wilmington, County of New Castle, Delaware 19808, USA.

Annex I

DATA PROCESSING ADDENDUM

This Data Processing Addendum (hereinafter: "**Addendum**") forms an inseparable part of the Privacy Policy of **GhostMonitor Inc.** (a private limited company operating under the laws of Delaware; registration number: 6088550; address: 251 Little Falls Drive, City of Wilmington, County of New Castle, Delaware 19808, USA; hereinafter: "**Data Processor**") and Principal Agreement (defined below). By accepting the terms of the Privacy Policy, the present data processing addendum becomes effective and it shall govern the data processing relationship between the Data Processor and the customer of Data Processor (hereinafter: "**Data Controller**") when processing personal data on behalf of the Data Controller (Data Processor and Data Controller together hereinafter: "**Parties**").

Preamble

In the context of provision of Data Processor's electronic services based on the contract concluded between Data Controller and Data Processor (hereinafter: "**Principal Agreement**"), the Data Processor will process the personal data as specified in Section IV of the present Addendum on behalf of the Data Controller.

The purpose of present Addendum is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation; hereinafter: "**GDPR**") for the transfer of personal data to a third country.

In connection with the personal data collected from individuals located within the European Union member countries, in accordance with the Article 28 of the GDPR, the Parties are obliged to record in writing their rights and obligations regarding their data processing relationship.

Except where the context requires otherwise, references in this Addendum to the Principal Agreement / Privacy Policy are to the Principal Agreement / Privacy Policy as amended by, and including, this Addendum.

I. DEFINITIONS

1. The capitalized terms used in this Addendum shall have the meanings set forth in this Addendum. Terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement / Privacy Policy. Except as modified below, the terms of the Principal Agreement / Privacy Policy shall remain in full force and effect.

2. Where these present Addendum uses the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in the GDPR.

3. The clauses of the Addendum shall be read and interpreted in the light of the provisions of the GDPR.

II. OBLIGATIONS OF THE PARTIES

1. DATA PROTECTION SAFEGUARDS

1.1 Instructions

1.1.1 The Data Processor shall process the personal data only on documented instructions from the Data Controller. The Data Controller may give further instructions regarding the data processing, within the framework the contract agreed with the Data Processor, throughout the duration of the contract, but such instructions shall always be documented.

1.1.2 The Data Processor shall immediately inform the Data Controller if it is unable to follow those instructions.

1.2 Purpose limitation

The Data Processor shall process the personal data only for the specific purposes of the transfer, as set out in Section IV of the present Addendum.

1.3 Transparency

The Parties shall provide the data subject with a copy of the Addendum upon request. This is notwithstanding the obligations of the Data Controller under Articles 13 and 14 of the GDPR, in particular to inform the data subject about the transfer of special categories of data.

1.4 Accuracy

If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay. In this case the Data Processor shall cooperate with the Data Controller to erase or rectify the data.

1.5 Storage limitation and erasure or return of data

Processing by the Data Processor shall only take place for the duration specified in the present Addendum. Upon termination of the provision of the processing services or the Principal Agreement, the Data Processor shall delete all personal data processed on behalf of the Data Controller and certify to the Data Controller that it has done so. This is notwithstanding any requirements under local law applicable to the Data Processor prohibiting return or destruction of the personal data. In that case, the Data Processor warrants that it will guarantee, to the extent possible, the level of protection required by as set forth in the present Addendum and will only process it to the extent and for as long as required under that local law.

1.6 Security of processing

1.6.1 The Data Processor and, during the transmission, also the Data Controller shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or

access to that data (hereinafter: "**Personal Data Breach**"). In assessing the appropriate level of security, they shall take due account of the risks involved in the processing, the nature of the personal data and the nature, scope, context and purposes of processing, and in particular consider encryption during transmission and anonymisation or pseudonymisation where this does not prevent fulfilling the purpose of processing. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall where possible remain under the exclusive control of the Data Controller. In complying with this obligation, the Data Processor shall implement the technical and organisational measures specified in Section V of the present Addendum.

1.6.2 The Data Processor shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the Principal Agreement. The Data Processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

1.6.3 In the event of a Personal Data Breach concerning personal data processed by the Data Processor, the Data Processor shall take appropriate measures to address the Personal Data Breach, including measures to mitigate its adverse effects. The Data Processor shall also notify the Data Controller without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to be taken to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall be provided subsequently as it becomes available without undue delay.

1.6.4 The Data Processor shall cooperate in good faith with and assist the Data Processor in any way necessary to enable the Data Processor to comply with its obligations under the GDPR, notably to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the Data Processor.

1.7 Special categories of personal data

To the extent the transfer includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "**Special Categories Of Data**"), the Data Processor shall apply the specific restrictions and/or additional safeguards described in Section IV.

1.8 Onward transfers

The Data Processor shall only disclose the personal data to a third party on the basis of documented instructions from the Data Controller. In addition, the data may only be disclosed to a third party located outside the European Union (hereinafter "**Onward Transfer**") if the third party is or agrees to be bound by the present Addendum or, alternatively, an Onward Transfer by the Data Processor may only take place if:

(a) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of the GDPR with respect to the processing in question;

(b) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of the GDPR that covers the Onward Transfer.

Any disclosure may only take place subject to compliance by the Data Processor with all the other safeguards under the present Addendum, in particular purpose limitation.

1.9 Documentation and compliance

1.9.1 The Data Processor shall promptly and properly deal with inquiries from the Data Controller that relate to the processing under the present Addendum.

1.9.2 The Parties shall be able to demonstrate compliance with the present Addendum. In particular, the Data Processor shall keep appropriate documentation on the processing activities on behalf of the Data Controller under its responsibility.

1.9.3 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations set out in the present Addendum and allow for and contribute to reviews of data files and documentation, or of audits of the processing activities covered by the present Addendum, in particular if there are indications of non-compliance. In deciding on a review or audit, the Data Controller may take into account relevant certifications held by the Data Processor.

1.9.4 The Data Controller may choose to conduct the audit by itself, to mandate, at its own cost, an independent auditor or to rely on an independent audit mandated by the Data Processor. Where the Data Processor mandates an audit, it has to bear the costs of the independent auditor. Audits may also include inspections at the premises of the Data Processor and shall be carried out with reasonable notice.

1.9.5 The Data Processor shall make the information referred to in the above paragraphs 1.9.2 and 1.9.3, including the results of any audits, available to the competent supervisory authority on request.

2. LOCAL LAWS AFFECTING COMPLIANCE WITH THE ADDENDUM

2.1 The Parties declare that they have no reason to believe that the laws in the third country of destination applicable to the processing of the personal data by the Data Processor, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Data Processor from fulfilling its obligations under the present Addendum. This is based on the understanding that laws that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR, are not in contradiction with the Addendum.

2.2 The Parties declare that they have taken due account in particular of the following elements:

(a) the specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the Data Processor for the type of data transferred;

(b) the laws of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities, as well as the applicable limitations and safeguards;

(c) any safeguards in addition to those under the Addendum, including the technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination.

2.3 The Data Processor warrants that, in carrying out the assessment under the above paragraph 2.2, it has made best efforts to provide the Data Controller with relevant information and agrees that it will continue to cooperate with the Data Controller in ensuring compliance with the present Addendum.

2.4 The Parties consider the present Addendum as the documentation of the assessment under the above paragraph 2.2, especially the content of Sections IV-V, and make it available to the competent supervisory authority upon request.

2.5 The Data Processor agrees to promptly notify the Data Controller if, after having agreed to the Addendum and for the duration of the Principal Agreement, it has reason to believe that it is or has become subject to laws that are not in line with the requirements under the above paragraph 2.1, including following a change of the laws in the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that are not in line with the requirements under the above paragraph 2.1.

2.6 Following a notification pursuant to the above paragraph 2.5, or if the Data Controller otherwise has reason to believe that the Data Processor can no longer fulfil its obligations as set forth in the Addendum, the Data Controller shall promptly identify appropriate measures (such as, for instance, technical or organisational measures to ensure security and confidentiality) to be adopted by the Data Controller and / or Data Processor to address the situation, if appropriate in consultation with the competent supervisory authority. If the Data Controller decides to continue the transfer, based on its assessment that these additional measures will allow the Data Processor to fulfil its obligations set forth in the present Addendum, the Data Controller shall forward the notification to the competent supervisory authority together with an explanation, including a description of the measures taken. The Data Controller shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the Data Controller shall inform the competent supervisory authority and shall be entitled to terminate the Principal Agreement. When the Principal Agreement is terminated pursuant to the present paragraph, clauses 1.4 and 1.5 of section III. shall apply.

3. OBLIGATIONS OF THE DATA PROCESSOR IN CASE OF GOVERNMENT ACCESS REQUESTS

3.1 Notification

3.1.1 The Data Processor agrees to promptly notify the Data Controller and, where possible, the data subject (if necessary, with the help of the Data Controller) if it:

(a) receives a legally binding request by a public authority under the laws of the country of destination for disclosure of personal data transferred pursuant to the present Addendum; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided;

(b) becomes aware of any direct access by public authorities to personal data transferred pursuant to the Addendum in accordance with the laws of the country of destination; such notification shall include all information available to the Data Processor.

3.1.2 If the Data Processor is prohibited from notifying the Data Controller and / or the data subject, the Data Processor agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicate as much information and as soon as possible. The Data Processor agrees to document its best efforts in order to be able to demonstrate them upon request of the Data Controller.

3.1.3 To the extent permissible under the laws of the country of destination, the Data Processor agrees to provide to the Data Processor, in regular intervals for the duration of the Principal Agreement, the greatest possible amount of relevant information on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.).

3.1.4 The Data Processor agrees to preserve the information pursuant to the above paragraphs 1.-3. for the duration of the Principal Agreement and make it available to the competent supervisory authority upon request.

3.1.5 The above paragraphs 3.1.1-3.1.3 are notwithstanding the obligation of the Data Processor pursuant to clause 1 of Section III to promptly inform the Data Controller where it is unable to comply with the clauses of the Addendum.

3.2 Review of legality and data minimization

3.2.1 The Data Processor agrees to review, under the laws of the country of destination, the legality of the request for disclosure, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if, after a careful assessment, it concludes that there are grounds under the laws of the country of destination to do so. When challenging a request, the Data Processor shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are notwithstanding the obligations of the Data Processor pursuant to clause 2.5 of Section II.

3.2.2 The Data Processor agrees to document its legal assessment as well as any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make it available to the Data Controller. It shall also make it available to the competent supervisory authority upon request.

3.2.3 The Data Processor agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

4. Use of sub-processors

4.1.1 The Data Processor shall not sub-contract any of its processing activities performed on behalf of the Data Controller under the present Addendum to a sub-processor without its prior specific written authorisation. The Data Processor shall submit the request for specific authorisation at least 8 days prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the Data Controller can be found in Section IV.

4.1.2 Where the Data Processor engages a sub-processor for carrying out specific processing activities (on behalf of the Data Controller), it shall do so by way of a written contract which provides for the same data protection obligations as the ones binding the Data Processor under the Addendum, including in terms of third party beneficiary rights for data subjects. The Parties agree that, by complying with this paragraph, the Data Processor fulfils its obligations under clause 1.8 of section II. The Data Processor shall ensure that the sub-processor complies with the obligations to which the Data Processor is subject pursuant to the present Addendum.

4.1.3 The Data Processor shall provide, at the Data Controller's request, a copy of such a sub-processor agreement and subsequent amendments to the Data Controller.

4.1.4 The Data Processor shall remain fully responsible to the Data Controller for the performance of the sub-processor's obligations under its contract with the Data Processor. The Data Processor shall notify the Data Controller of any failure by the sub-processor to fulfil its obligations under that contract.

4.1.5 The Data Processor shall agree a third party beneficiary clause with the sub-processor whereby, in the event of bankruptcy of the Data Processor, the Data Controller shall be a third party beneficiary to the sub-processor contract and shall have the right to enforce the contract against the sub-processor, including where applicable by instructing the sub-processor to erase or return the personal data.

5. DATA SUBJECT RIGHTS

5.1 The Data Processor shall promptly notify the Data Controller about any inquiry or request received directly from a data subject. It shall not respond to that inquiry or request itself unless and until it has been authorised to do so by the Data Controller.

5.2 Taking into account the nature of the processing, the Data Processor shall assist the Data Controller in fulfilling its obligations to respond to data subjects' inquiries and requests for the exercise of their rights under the GDPR.

5.3 The data subjects may invoke and enforce the clauses set forth in the present Addendum as third party beneficiaries, against the Data Controller and / or Data Processor, with the following exceptions:

(a) Section I;

(b) Section II: clauses 1.9.1, 1.9.3, 1.9.4, 1.9.5, 3.1.3, 3.1.4, 3.1.5, 4, 7.1, 7.2; 8., and 9.;

(c) Section III: clauses 1., 3.1, 3.2 and 5.

6. REDRESS

6.1 The Data Processor shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints or requests. It shall promptly deal with any complaints or requests by a data subject.

6.2 The Parties agree that if there is a dispute between a data subject and one of the Parties as regards compliance with the Addendum, they shall keep each other informed about such proceedings and, where appropriate, cooperate in resolving the issue in a timely fashion.

6.3 Where the dispute is not amicably resolved and the data subject invokes a third-party beneficiary right pursuant to clause 4.3 of section II., the Data Processor accepts the decision of the data subject to:

(a) lodge a complaint with the competent supervisory authority within the meaning of clause 8 of section II.;

(b) refer the dispute to the competent courts within the meaning of clause 3 of section III.

6.4 The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of the GDPR.

6.5 The Data Processor accepts to abide by a decision binding under the applicable EU / Member State law.

6.6 The Data Processor agrees that the choice made by the data subject will not prejudice his / her substantive and procedural rights to seek remedies in accordance with applicable laws.

7. LIABILITY

7.1 Each Party shall be liable to the other Party for any material or non-material damages it causes the other Party by any breach of the clauses set forth in the present Addendum.

7.2 Liability as between the Parties is limited to actual damage suffered. Punitive damages are excluded.

7.3 The Data Processor shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the Data Processor causes the data subject for any breach of the third party beneficiary rights under the present Addendum.

7.4 The Data Controller shall be responsible for ensuring that the Processing of Personal Data takes place in compliance of the GDPR and for ensuring that the processing of personal data which the Data Processor is instructed to perform has a legal basis.

7.5 Parties agree that Data Controller is solely obliged to inform its customers by providing the necessary information prescribed by article 14 of the GDPR.

7.6 Data Processor hereby excludes any and all liability regarding the information regulated by the present section and excludes any liability for any financial and/or non-material loss and/or damage, consequential loss and/or damages, and loss of profit may occur because of the failure of the Data Controller to perform its obligation to inform its customers and/or failed to perform its obligations as described in the present Addendum.

7.7 Data Controller is obliged to reimburse and indemnify Data Processor if any financial and/or non-material loss and/or damage, consequential loss and/or damage, and loss of profit occur at the Data Processor due to the infringement of any of the obligations prescribed in the present Addendum

7.8 The Data Controller shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the Data Controller or the Data Processor causes the data subject for any breach of the third party beneficiary rights under the Addendum. This is without prejudice to the liability of the Data Controller and, where the Data Controller is a processor acting on behalf of a controller, the controller under the GDPR.

7.9 Where more than one Party is responsible for any damage caused to the data subject resulting from a breach of the Addendum, both Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against either of these Parties.

7.10 The Data Processor may not invoke the conduct of a sub-processor to avoid its own liability.

8. INDEMNIFICATION

8.1 The Parties agree that if one Party is held jointly and severally liable for a breach of the Addendum together with another Party, it is entitled to claim back as indemnification that part of the liability that corresponds to the other Party's part of responsibility.

8.2 Indemnification is contingent upon the Party to be indemnified:

(a) promptly notifying the other Party of a claim, and

(b) providing reasonable cooperation and assistance to the other Party in defense of such claim.

9. SUPERVISION

9.1 The supervisory authority with responsibility for ensuring compliance by the Data Processor with the GDPR as regards the data transfer, namely the Nemzeti Adatvédelmi és Információszabadság Hatóság of Hungary, shall act as competent supervisory authority.

III. FINAL PROVISIONS

1. NON-COMPLIANCE WITH THE CLAUSES AND TERMINATION

1.1 The Data Processor shall promptly inform the Data Controller if it is unable to comply with the Addendum, for whatever reason.

1.2 In the event that the Data Processor is in breach of the Addendum or unable to comply with the Addendum, the Data Controller shall suspend the transfer of personal data to the Data Processor until compliance is again ensured or the Principal Agreement is terminated. This is notwithstanding clause 2.6 of section II.

1.3 The Data Controller shall be entitled to terminate the Principal Agreement where:

(a) the Data Controller has suspended the transfer of personal data to the Data Processor pursuant to the paragraph 1.2 of section III. and compliance with the Addendum is not restored within a reasonable time and in any event within one month,

(b) the Data Processor is in substantial or persistent breach of the Addendum, or

(c) the Data Processor fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations under the Addendum.

In this case, it shall inform the competent supervisory authority of such non-compliance.

1.4 Personal data that has already been transferred prior to the termination of the Principal Agreement shall at the choice of the Data Controller immediately be returned to the Data Controller or destroyed in their entirety. The same shall apply to any copies of the data. The Data Processor shall certify the destruction of the data to the Data Controller. These obligations are notwithstanding any requirements under local law applicable to the Data Processor that prohibits return or destruction of the personal data transferred. In that case, the Data Processor warrants that it will ensure, to the extent possible, the level of protection required by the Addendum and will only process the data to the extent and for as long as required under that local law.

1.5 Either Party may revoke its agreement to be bound by the present Addendum where (i) the European Commission adopts a decision pursuant to Article 45(3) of the GDPR that covers the transfer of personal data to which the present Addendum applies; or (ii) the GDPR becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under the GDPR.

2. GOVERNING LAW

The present Addendum shall be governed by the law of one of the Member States of the European Union, provided such law allows for third party beneficiary rights. The Parties agree that this shall be the law of Hungary.

3. CHOICE OF FORUM AND JURISDICTION

3.1 Any dispute arising from the Addendum shall be resolved by the courts of a Member State of the European Union. The Parties agree to submit themselves to the jurisdiction of such courts.

3.2 The Parties agree that those shall be the courts of Hungary.

3.3 Legal proceedings by a data subject against the Data Controller and / or Data Processor may also be brought before the courts of the Member State where the data subject has his or her habitual residence.

4. HIERARCHY

In the event of a conflict between the clauses of the present Addendum and the provisions of any other existing agreement that are agreed or entered into thereafter between the Parties, the clauses of the Addendum shall prevail.

IV. DESCRIPTION OF THE TRANSFER

1. Categories of data subjects whose personal data is transferred to Data Processor

The customers of the Data Controller, who are about to place an order or already placed an order on the Data Controller's website.

2. Categories of personal data transferred to Data Processor

First name, last name, birth date, location, IP address, e-mail address, address, phone number.

3. Purposes of the data transfer and further processing

To provide the Services to Data Controller.

4. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The transferred personal data is being processed by the Data Processor until it is necessary for the Data Processor to provide the Services, prescribed by law or necessary for the legitimate interest of the Data Processor. The Data Processor uses the services of the subprocessors listed in section 6.2 of the Policy.

V. TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. INTERNAL SECURITY AT DATA PROCESSOR

1.1 The offices of Data Processor are secured by keycard access and the entrances are monitored with video cameras and with security staff present.

1.2 All employees of Data Processor sign a document, which outlines their responsibility in protecting customer and data subject data.

2. SOFTWARE LEVEL SECURITY OF DATA PROCESSOR

2.1 Data Processor shall have DDOS mitigation in place at all of their data centers.

2.2 All databases of Data Processor are kept separate and dedicated to preventing corruption and overlap. Data Processor has multiple layers of logic that segregate user accounts and data subjects' information from each other.

2.3 Data Processor encrypts all data stored on its servers.