PRIVACY POLICY

Last modified: August 30, 2022

This Privacy Policy (the "Policy") explains how Ghostmonitor Inc. dba Recart ("Recart", "Recart", "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 Standard Contractual Clauses attached to the present Policy as *Schedule 1* (hereinafter: "SCC"), 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 SCC. If you do not agree with this Policy, the SCC or our practices, you may not use our Website or our services, including any testing feature on the Website (the "Services"). This Policy may change from time to time and is incorporated into our Website Terms of Service. 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 Recart 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 Recart 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 Recart 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, Recart shall be deemed as data controller.

By using the Services of Recart – as described under section 2.3 of the present Policy – you as our user shall be deemed as a data controller and Recart shall be considered as a data processor. The rights and obligations regarding to that relationship between you as data controller and Recart as data processor is governed by the SCC attached to the present Policy as *Schedule 1*.
Recart may from time to time handle personal data collected from individuals located within the European Union ("EU") member countries. Consistent with GDPR Recart 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, Recart 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. Recart 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 Recart's certification, please visit https://www.privacyshield.gov.

Recart 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 Recart's treatment of information that Recart gathers when you are accessing Recart's Website as a user and when you use Recart Services. Also, this Policy covers Recart's treatment of your information that Recart shares with Recart's business partners. This Policy does not apply to the practices

of third parties that Recart does not own or control (such as third-party websites that you may access from the Website), or to individuals that Recart does not employ or manage.

2. What information does Recart collect?

The information we gather from users enables Recart 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. Recart 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, Recart provides you a written contract on data processing, therefore, the data processing relationship between you, as a data controller and Recart, as a data processor shall be governed by the SCC attached to the present Policy as *Schedule 1*, 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 Recart 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 Recart 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

For our testing feature, we also collect the following information in addition to some of the items identified above:

- Store name
- Store url

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 anonymous 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

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**: Recart 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**: Recart 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 Recart 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 Recart.

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. Until a new adequacy decision between the EU and the U.S. comes into effect, temporarily these data transfers rely on Article 49

(1) (b). Recart 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 Recart 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:

Recart 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 Recart 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.

Recart 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 Recart 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 Recart 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. Recart 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 Recart 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.

Schedule I

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. 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 exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter 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 address the breach including, where appropriate, measures 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, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular 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 importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, 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 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(i) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(ii) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(iii) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(iv) he data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(v) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least *3 calendar days* in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer 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. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) 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 Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer 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.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer 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 importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter 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 exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices 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 Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter 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 exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

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

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as

possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimization**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 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 Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Hungary.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Hungary.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter:

1. Name:

   The legal entity as set out in the order signed by the data exporter and the data importer (hereinafter: "Order").

   Address: **As set out in the Order.**

   Activities relevant to the data transferred under these Clauses:

   Using messaging for product and service marketing services as set out in the Order and in the Terms of Service referred to in the Order.

   Signature and date: **Date as per the Order.**

   Role (controller/processor): **Controller**.

Data importer:

1. Name: **Ghostmonitor Inc.**

   Address:

   251 Little Falls Drive, City of Wilmington, County of New Castle, Delaware 19808, USA

   Contact person's name, position and contact details:
   David Toth, Head of Operations, e-mail: gdpr@recart.com

   Activities relevant to the data transferred under these Clauses:

   Using messaging for product and service marketing as set out in the Order and in the Terms of Service referred to in the Order.

   Signature and date: **Date as per the Order.**

   Role (controller/processor): **Processor.**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The data exporter's customers who are about to place an order or already placed an order on the data exporter's website.

Categories of personal data transferred
First name, last name, birth date, location, IP address, e-mail address, address, phone number.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
The data is transferred on a continuous basis.

Nature of the processing

The processing of personal data referred to under these Standard Contractual Clauses shall occur throughout the term of this Standard Contractual Clauses and the provision of the messaging for product and service marketing services.

Purpose(s) of the data transfer and further processing

To provide messaging for product and service marketing services as described in the Order and in the Terms of Service referred to in the Order.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The personal data will be retained until it is necessary for the data importer to provide its services, or until it is prescribed by law.

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

The data exporter determines the subject matter, nature, and duration of processing of persona data transferred to sub-processor(s).

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority shall be identified by choosing the applicable option specified in Paragraph a) of Clause 13. Contact data of the EU national data protection authorities are available at: https://edpb.europa.eu/about-edpb/about-edpb/members_en

---

ANNEX II

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

1. **Measures for internal IT and IT security governance and management**

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

1.2 All employees of the data importer sign a document which outlines their responsibility in protecting customer and data subject data and receive training in data protection.

1.3 All employees of the data importer have a personal user account to access the computers of the data importer with a strong password in place. The data importer has proper HR management in place, therefore every user account granting access to the IT infrastructure is deleted upon the quitting of an employee.

1.4 The data importer ensures the regular maintenance of its IT infrastructure.

2. **Software level security of data importer**

2.1 The data importer shall have DDOS mitigation in place at all of their data centers.

2.2 All databases of data importer are kept separate and dedicated to preventing corruption and overlap.

2.3 The data importer logs events of the data processing electronically.

3. **Data minimisation**

3.1 The data importer only receives and processes personal data that are required for the provision of the services.