DATA PROCESSING AGREEMENT
(„AGREEMENT”)

entered into on 04-01-2019 by and between

GetResponse Sp. z o.o. with its registered office in Gdańsk (80-387), Arkońska 6, A3, entered in theRegister of Enterprises of the National Court Register kept by the District Court for Gdańsk-Północ in Gdańsk, 7thCommercial Division of the National Court Register, at KRS No. 0000187388, with NIP No.9581468984, REGON No.192998251, with a share capital of PLN 5.559.840 represented by: Daniel Brzeziński –Vice president, hereinafter: **„GetResponse”**

and

FitKit International with its registered office in Vangel Todorovski 5/1-30, Skopje, Aerodrom, 1000, Republic of Macedonia represented by: Josif Damjanov, Co-founder hereinafter: **„Customer”**

The Customer and GetResponse are hereinafter also jointly referred to as **„Parties”** and each separately as a **„Party”**.

Whereas:

1. The service provided by GetResponse to the Customer (**"Service"**) may require GetResponse to process Personal Data (as defined below), the Parties wish to ensure that the Personal Data processing is in conformity with the applicable laws, in particular with 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, and repealing Directive 95/46/EC (**"GDPR"**) - from the moment it shall apply - and with other applicable personal data protection laws;

2. The Customer is the controller of the personal data processed in the course of using the Service ("Personal Data") or acts as a processor, based on an authorization granted by the Personal Data controller and on behalf of the controller. The detailed scope of Personal Data and the categories of data subjects are defined in **Annex 1;**

3. GetResponse provides the Service to the Customer based on the GetResponse Terms of Service (**"Terms of Service"**) with this Agreement constituting an integral part thereof.

The Parties have decided as follows:

§ 1 SUBJECT MATTER OF THE AGREEMENT

1. Pursuant to Article 28(3) of the GDPR,the Customer engages GetResponse in processing of the Personal Data and GetResponse hereby accepts the processing.

2. GetResponse shall process the Personal Data: (i) in accordance with applicable laws and the Agreement, (ii) exclusively for the purpose of providing the Service to the Customer by GetResponse, (iii) to the extent defined in **Annex 1** and (iv) in the period from the commencement of Service provision to Agreement termination, subject to §7(2)hereof.

3. The role of GetResponse shall be limited to providing the Customer with the Service tools to be used for the purpose of Personal Data processing. GetResponse does not have any impact on the scope of the Personal Data processed by the Customer in the Service,except for specifying the minimum scope of the Personal Data required for the proper use of the Service, GetResponse does not determine the purposes and means of processing, does not monitor the scope of these data or the lawfulness of the basis for their processing, nor does it check if the Customer processes them correctly.

§2 REPRESENTATIONS OF THE CUSTOMER

1. The Customer hereby represents that it has obtained and that it processesPersonal Data in accordance with applicable laws, including GDPR. The Customer confirms in particular that it has: (i) obtained and holds the legally required direct marketing consents, including consents to send commercial information by e-mail or telephone and to use telecommunications terminal equipment and automated phone call systems for direct marketing purposes –if the Customer carries out such activities, (ii) informed the data subjects about the processing of the data to the extent and in a manner required under the GDPR, (iii) has the right to process Personal Data and engage GetResponse for carrying out processing activities to the extent and for the purpose defined in **Annex 1** hereto. Notwithstanding the foregoing, if the Customer is not the Personal Data controller, it confirms that it has received the permission of the respective controller as required under the GDPR to engage GetResponse for carrying out processing for the purpose and to the extent in question.

2. The Customer hereby confirms that the technical and organizational measures implemented by GetResponse and defined in **Annex 2** are suitable and sufficient for the protection of the rights of data subjects, and the Customer considers GetResponse to be providing sufficient guarantees in this respect.

3. Notwithstanding the foregoing,the Customer shall use the Service in a safe manner and in accordance with the law, which includes properly securing the Customer account authentication data, ensuring the security of the Personal Data while providing them for the purpose of the Service, taking suitable actions to ensure secure encryption or creation of internal backup of the Personal Data entrusted to GetResponse and ensuring protection against unauthorized access.The Customer hereby acknowledges and accepts that in connection with the Service GetResponse uses cookies and other similar technologies to track user activity. The Customer undertakes to apply appropriate notices, obtain appropriate consents and have mechanisms for their withdrawal (opt-in and opt-out) required by law to enable GetResponse to use these technologies lawfully and collect data from the Contacts' devices in accordance with Cookie Policy available at https://www.getresponse.com/legal/cookie-policy.html and in a manner describer therein.

4. The Customer shall inform GetResponse without undue delay about any inspection performed by the Inspector General for the Protection of Personal Data (**"IGPPD"**), and from the moment of its appointment -President of the Personal Data Protection Authority (**"PPDPA"**) that is connected with the processing of the Personal Data entrusted to GetResponse and about any notice from the IGPPD or PPDPA requesting explanations regarding the same.

§3 THE CUSTOMER'S INSTRUCTIONS

1. GetResponse shall process the Personal Data exclusively in line with the instructions from the Customer, unless the European Union or Member State law requires otherwise. In the latter case, §4(6)(a) hereof shall apply.

2. The Customer's instructions are given in the Agreement or can be given and followed through the functionalities provided by GetResponse in the Service. The Customer shall make sure that any instructions given to GetResponse are in conformity with applicable data protection laws.

3. Any further instructions that go beyond the instructions defined in §3(2) above must pertain to the subject matter of the Agreement or the subject matter of the Service provided in accordance with Terms of Service. If executing further instructions results in costs for GetResponse, GetResponse shall inform the Customer about such costs, explaining the amounts of the costs, before executingthe instruction. Only uponthe Customer'sconfirmationof bearingthesecosts and their payment is GetResponse obliged to execute further instruction, provided that technical and organisational measures allow it. The Customer shall give further instructions in writing, unless urgency or other special circumstances justify giving instructions through electronic means of communication. Instructions in any form other than in writing should be subsequently properly documented without undue delay.

4. GetResponse shall immediately inform the Customer if GetResponse believes that an instruction infringes the GDPR or other European Union or Member State data protection provisions, and shall request the Customer to withdraw, change or confirm the challenged instruction. While waiting for the Customer's decision, GetResponse has the right to suspend the performance of the challenged instruction. If, despite the Customer's explanation,executing the challenged instruction would infringe the GDPR or other European Union or Member State data protection provisions, GetResponse has the right to refrain from executing the instruction.

§4 REPRESENTATIONS AND OBLIGATIONS OF GETRESPONSE

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks for rights and freedoms of natural persons, GetResponse hereby represents that as per Article 32 of the GDPR, GetResponse has implemented appropriate technical and organizational measures to secure the processing of Personal Data. The description of the implemented measures is available in **Annex 2**. GetResponse may at any time change the implemented measures, provided that the protection level they ensure is not lower than that ensured by the measures applicable at the conclusion of the Agreement. The Customer can find an information about the current

technical and organizational measures along with an information about any changes to the scope of the implemented measures in the Account.

2. As a justified request of the Customer, GetResponse shall make available to the Customer any further information necessary to demonstrate its compliance with the obligations laid down in Article 28 of the GDPR. The last sentence of §4(5) hereof shall apply as appropriate.

3. GetResponse shall ensure appropriate security of the Personal Data against unauthorized access and unauthorized seizure, as well as against damage, destruction or loss, and shall take any necessary steps as required by law to keep the Personal Data and how they are secured confidential.

4. GetResponse hereby represents that all persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality as per Article 28(3)(b) of the GDPR, and GetResponse shall be liable for their acts or omissions as for its own acts or omissions.

5. It is the responsibility of the Customer to satisfy the requests of Personal Data subjects and to prepare replies to such requests. GetResponse shall reasonably support the Customer to the best of its abilities and to a reasonable extent, in fulfilling its obligations, in particular through the application of appropriate technical and organizational measures necessary for the Customer to support the exercise of the data subjects' rights under the GDPR.

6. GetResponse shall assist the Customer in compliance with the obligations pursuant to Articles 32 to 36 of the GDPR in respect of the Service by providing the Customer with the necessary information. In respect of assisting the Customer in data protection impact assessment (Article 35 of the GDPR) and in prior consultation with the supervisory authority (Article 36 of the GDPR), GetResponse shall assist only insofar as the Customer is unable to fulfill its obligations by other means. GetResponse shall inform the Customer about the costs of such assistance. Once the Customer confirms that it will cover such costs, GetResponse shall provide the required assistance.

7. GetResponse shall inform the Customer without undue delay upon receiving any credible and confirmed information:

    a. that GetResponse or its sub-processors have been obliged, under the European Union or Member State law to which GetResponse is subject, to process the Personal Data in a manner going beyond the Customer's instructions; in such a case, GetResponse shall inform the Customer of such obligation before processing, unless law prohibits providing such information on important grounds of public interest; in such an event, the notice to the Customer shall specify the legal requirement arising from the European Union or Member State law;

    b. about any identified Personal Data breach committed by GetResponse or its sub-processor that affects the Customer's Personal Data hereunder. In such a case, GetResponse shall support the Customer in the Customer's fulfilment, where applicable, of an obligation to notify the supervisory authority or the data subject by providing the information available to GetResponse in accordance with Article 33(3) of the GDPR.

§5 USE OF SUB-PROCESSORS (ENGAGEMENT OF OTHER PROCESSORS)

1. To ensure proper provision of the Service, the Customer authorizes GetResponse to engage other processors for carrying out processing activities. For the avoidance of doubt and without limiting the general authorisation granted to GetResponse in the preceding sentence, the Customer in particular agrees to the sub-processors listed in **Annex 3.**

2. The current list of GetResponse's sub-processors is available in the Customer's Account. GetResponse shall inform the Customer about any intended changes concerning the addition or replacement of other processors. The Customer shall be informed about this through a notice in the Customer's Account and properly in advance. The Customer shall have the opportunity to object (via electronic means of communication or by post) to such changes within 14 days of receiving a notice on the intended change. If the Customer does not object within 14 days of receiving the information about the intended change, the Customer is deemed to have agreed to the change. Having received an objection, GetResponse has 30 days to determine how to proceed in relation to the objection. On the expiry of that period, each Party may terminate the Agreement in line with the provisions of the Service Agreement. Notwithstanding the foregoing, GetResponse stipulates that the Customer's objection to a chosen sub-processor may render the Customer unable to use all the functionalities of the Service.

3. Engagement of other processors may only take place within the limits of and for the purpose of performing the Service. GetResponse hereby represents that (i) the sub-processors it has engaged meet all the requirements arising from the GDPR and from applicable data protection provisions, (ii) it has entered into Personal Data processing agreements with the sub-processors as required under Article 28(4) of the GDPR and that such agreements include provisions imposing obligations analogical to those defined in the Agreement in respect of GetResponse, and that (iii) the personal data protection standard followed by the sub-processors is at least equal to the personal data protection standard followed by GetResponse. If sub-processor chosen by GetResponse is located in a third country within the meaning of GDPR, GetResponse shall be obliged to ensure that the conditions set in Chapter V of the GDPR are met.

§6 CUSTOMER'S RIGHTS TO AUDIT

1. The Customer shall have the right to audit GetResponse's compliance with the Agreement in terms of Personal Data processing (**"Audit"**). An Audit may also be conducted by an independent auditor mandated by the Customer, subject to prior conclusion of confidentiality agreement between the auditor and GetResponse.

2. The Customer shall not appoint as an auditor any entity conducting directly or indirectly competitive activity in relation to activity conducted by GetResponse. Competitive activity shall mean any activity, whether or not fee-based, irrespective of the place and territory where it is carried out, regardless of the legal form, conducted in the same or the same subject range and addressed to the same group of recipients, coinciding - even partially - with the scope of the main or the side activity of GetResponse or of entities from the GetResponse group worldwide. Assessment of whether an entity is a competitor will include not only the subject of business activity of such an entity as listed in its articles of association or other document constituting the basis for its functioning, but also any activities actually

pursued by that entity. If the Audit is mandated to GetResponse's competitors, GetResponse shall have the right to refuse to allow the Audit until another entity is mandated to carry out the Audit on behalf of the Customer or until the Parties agree on how to further proceed.

3. The Audit shall be subject to the following conditions: (i) it may only apply to the Personal Data entrusted to GetResponse for processing under the Agreement, it shall be limited to GetResponse's registered office, devices used to process the Personal Data and staff involved in the processing hereunder; (ii) it shall be carried out efficiently and as quickly as possible, taking no more than 2 working days, (iii) it shall not take place more than once a year, unless it is required under applicable laws or by a competent supervisory authority or takes place promptly after a material breach of the Personal Data processed hereunder is identified, (iv) it may take place during regular working hours of GetResponse, in a manner that does not disrupt GetResponse's business and is in conformity with GetResponse's security policies; (v) the Customer shall inform GetResponse about the intention to carry out the Audit via electronic means of communication or by post at least 14 working days before the intended Audit date. If an Audit cannot be carried out as intended for reasons beyond GetResponse's control or if other unexpected obstacles arise, GetResponse shall inform the Customer about such circumstances and shall suggest a new Audit date, which shall not be later than 7 working days after the date specified by the Customer; (vi) the Customer shall bear all costs arising from or connected with an Audit, except where an Audit reveals a serious breach of Personal Data security rules that pertains or is a threat to the Customer's Personal Data; (vii) an Audit cannot be intended or lead to the disclosure of legally protected secrets (including GetResponse's trade secrets). The Customer shall create an Audit report that summarizes the Audit findings. The report shall be submitted to GetResponse and shall represent GetResponse's confidential information which cannot be disclosed to any third parties without GetResponse's written permission unless this is required by the applicable laws.

4. If GetResponse adheres to an approved certification mechanism referred to in Article 42 of the GDPR or an approved code of conduct referred to in Article 40 of the GDPR, the Customer's auditing rights may also be exercised through GetResponse's reference to the results of the monitoring of the rules of certification or the code of conduct. If this is the case, the Audit shall only address issues that cannot be sufficiently clarified through the submission of such results by GetResponse.

§7 RETURN OR DELETION OF PERSONAL DATA

1. If the Agreement is terminated, GetResponse shall, according to the Customer's statement, delete the Personal Data (by deleting any existing copies of Personal Data) or return them to the Customer (along with any media where they are stored, if possible), unless GetResponse has the right to further process the Personal Data for a longer period based on independent legal grounds. If GetResponse does not receive the statement referred to in the preceding sentence, whether in writing or by e-mail, within 5 days of Agreement termination, the Customer shall be deemed to require that the entrusted Personal Data be deleted. If the Customer chooses to have the Personal Data returned, GetResponse shall provide the same to the Customer or enable the Customer to download the Personal Data in a commonly used and machine-readable format.

2. The Customer may obtain a copy of the processed Personal Data throughout the term of the Service Agreement, but no later than 60 days after the Customer's Account has been deactivated. In the said period of 60 days after the Customer's Account has been deactivated, the Personal Data shall only be processed by GetResponse for the purpose of potential reactivation of the Customer's Account, and shall only involve Personal Data storage for the

Customer without any other processing activities, subject to GetResponse's other obligations or rights arising from applicable laws or public authorities'' orders. After the expiry of this term, Personal Data shall be deleted from the main base without possibility of recovery. In the period of next 120 days Personal Data shall be subject to encryption and stored in backup copies only. The said 120-day period is required to delete the Personal Data completely due to specifics of the backup copies operations.

§8 LIABILITY

1. GetResponse's liability in contract and in tort shall be limited to direct actual losses incurred by the Customer. GetResponse shall not be liable for lost profit, notwithstanding the source, except where this is caused by wilful misconduct or gross negligence.

2. GetResponse's total liability, notwithstanding the number of and grounds for the Customer's claims, shall be limited to equivalent of amount payable for the Service for three settlement periods (settlement period shall mean, respectively, monthly period or 30 days) paid by the Customer in the settlement period immediately preceding the date when the event causing the damage occurred, with the exclusion of any amounts representing setup fees or any extra charges. The Customer hereby releases GetResponse from any liability above that limit.

3. GetResponse shall not be liable for not performing or improperly performing the Agreement resulting from Force Majeure.

4. The Parties agree that the Customer shall be liable for satisfying any and all claims of Personal Data subjects in connection with any damage arising from improper processing of personal data hereunder, unless the Customer demonstrates that the damage resulted from the sole through fault of GetResponse or GetResponse's sub-processors. If the Customer fails to demonstrate this, the Customer shall unconditionally indemnify GetResponse and hold it harmless in respect of any claims filed by the entities whose Personal Data GetResponse has processed based on the Agreement, and in connection with the processing of such data hereunder. If action is brought against GetResponse, the Customer shall, if so required by GetResponse, join the proceedings as a party and assume full liability for the claim.

§9 MISCELLANEOUS

1. The Parties jointly agree that save as otherwise provided in the Agreement, GetResponse's remuneration for the activities hereunder is included in the remuneration due for the provision of the Service to the Customer.

2. The Agreement has been concluded for an indefinite period, but it shall be terminated no later than on the day of return or deletion of Personal Data according to §7 hereof.

3. The Agreement shall supersede any arrangements between the Parties in respect of entrusting Personal Data which the Parties may have made before in connection with the Service, notwithstanding the form of such arrangements.

4. Any amendments to the Agreement shall be made in writing, including electronic means of communication.

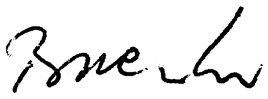
5. Any communications between the Parties shall be sent to the following addresses only:

    a. GetResponse – privacy@getresponse.com

    b. Customer - email address josif.damjanov@gmail.com

6. The Agreement shall be governed by Polish law. To any matters not regulated herein, the provisions of the GDPR, other applicable Polish laws, the Privacy Policy available at https://www.getresponse.com/legal/privacy.html and Terms of Service available at https://www.getresponse.com/legal shall apply. Any capitalized terms (e.g. Contacts, Force Majeure etc.) not defined herein shall have the meaning as assigned to them in Terms of Service. In the event of any discrepancies between Terms of Service and this Agreement, the provisions of this Agreement in relation to personal data protection shall prevail.

7. The Agreement has been executed in two counterparts, one for each Party.

GetResponse	Customer
	Josif Damjanov, Co-founder

Annex 1 – Description of Personal Data processing

1. Purpose of the Personal Data processing

Personal Data shall be processed by GetResponse in order for the Customer to use the Service provided by GetResponse.

2. Nature of the processing and the processing activities

Processing is both automated and non-automated. Personal Data processing by GetResponse takes place using the IT systems provided within the Service and includes following processing activities: collection, recording, storage, adaptation, alteration, disclosure, backuping Personal Data, as well as other activities as required to provide the Service.

GetResponse shall not communicate directly with the Personal Data subjects in the course of Personal Data processin

GetResponse's role is limited to making the Service tools available to the Customer for use in order to process the Personal Data. GetResponse does not have any impact on the scope of Personal Data processed by the Customer within the Service, does not determine the purposes and means of their processing and does not monitor scope of such Data.

3. Categories of data subjects

The Customer engages GetResponse in processing of the Personal Data of following categories of data subjects:

a. Contacts – including persons whose Personal Data are on the Contact List; or whose Personal Data is collected and stored using the Service; or to which the Customer will send communication using the Service, in particular contractors, customers, prospects, employees, contacts of the Customer's business partners, subscriber of the Customer's newsletter;
b. participants of webinars;
c. persons whose data is collected through forms and surveys;
d. persons authorized by the Customer to use the Account (Collaborators).

As a rule, the Service is not intended to process special categories of personal data referred to in Article 9 of the GDPR, personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR, nor personal data of children. However, decision as to the scope of data that to be processed by GetResponse in the Service belongs to the Customer. By using the Service to process such data, the Customer confirms that security measures implemented by GetResponse are in his opinion sufficient to protect entrusted Personal Data.

4. Categories of Personal Data to be processed

The Customer engages GetResponse for processing of following categories of Personal Data:

a. regarding Contacts: e-mail address.

The Service also allows for the processing of other information such as:

- first and last name
- company phone number, private phone number, mobile phone number, fax number
- URL address of the website through which Contact provided its data to the Customer
- the Contact's address details
- address of the website from which the Customer was redirected [http_referer]
- gender, age, date of birth
- workplace
- Personal Data contained in contents sent by the Customer with the use of the Service
- additional information about the Contact [comment] and other information based on fields defined by the Customer when collecting the Contacts' data from forms or surveys.

b. regarding participants of webinars: email address.

The Service also allows for the processing of other information such as:

- first and last name,
- nickname
- address of the website from which the participant was redirected [http_referer]
- additional information about the webinar participant collected by the Customer from registration form, during webinar or chat.

c. regarding persons whose data is collected through forms and surveys: email address.

The Service also allows for the processing of other information such as:

- first and last name,
- additional information based on the fields defined by the Customer.

d. regarding Collaborators of the Customer: email address, name of user.

e. regarding all above categories: data processed automatically while the Service is being used (data about the use of the Service; data collected using cookies or other technologies used to track users activity; IP data of the device from which the Contact was imported to the Customer's Contact List or on which the Contact opened an email sent to him by the Customer as part of using the Service; location data; data about the web browser).

Annex 2 – Description of the implemented organizational and technical measures for personal data protection

A. Organizational security measures.

I. Information Security Management System.

1. A general security policy has been developed, along with specific security policies regarding organization security, information security, IT system security and security of people and property, all of them defining the basic objectives of the actions related to implementation of the policies.
2. General and specific security standards have been defined that implement the assumptions of the security policies in terms of information security, IT system security, and security of people and property.
3. Specific procedures and operating instructions have been developed for the implementation of the security standards in terms of information security, IT system security, and security of people and property.
4. The policies, standards, procedures, and instructions are subject to periodic reviews and revisions, to be approved by the Company's top management.
5. A system to monitor changes in personal data processing legislation has been developed and put in place, and the continuity of its operations has been ensured.

II. Roles and tasks.

1. The roles and tasks in security management processes have been defined. The individuals responsible for compliance with each respective security policy have been appointed.
2. For every resource (whether physical or electronic) that is of value for the organization, a responsible person (Resource Owner) has been appointed as being in charge of managing the security of that resource.
3. To ensure proper level of personal data protection, an independent Data Security Administrator, which, from the date the GDPR shall apply, will be replaced by Data Protection Officer, has been designated and appointed.
4. The Data Security Administrator, and subsequently the Data Protection Officer answers directly to the Company's top management.
5. The Data Security Administrator, and subsequently the Data Protection Officer has been included in all the processes connected with personal data processing.
6. The Data Security Administrator, and subsequently the Data Protection Officer has been granted sufficient access to any and all information and documentation connected with personal data processing.
7. Those who process personal data at the request and on behalf of the Company have been specifically indicated by name as authorized to process personal data.
8. All the individuals authorized to process personal data have been included in the internal personal data security and protection training scheme.
9. All the individuals authorized to process personal data have been obliged to respect data confidentiality throughout the term of employment and thereafter.

III. Access rights management

1. Access rights management procedures have been developed for access to data storage devices, rooms, zones, buildings, IT systems and elements of the IT infrastructure and network.
2. It has been assured that the individuals authorized to process personal data are assigned with minimum access rights, depending on the performed tasks.
3. A procedure of monitoring and checking the access rights ad hoc and periodically has been provided.
4. It has been assured that keys, access codes and access rights in the access control system for access to buildings, zones, rooms or part of rooms where personal data is processed are provided to individuals authorized to process personal data in accordance with the scope of the authorization and the scope of tasks performed within the job position.
5. It has been assured that buildings, zones, rooms or parts of rooms where personal data is processed are secured against unauthorized access in the absence of the individuals authorized to be in these rooms. Anyone who is not authorized to be in the rooms used for personal data processing may only stay there under the supervision of authorized persons.
6. A process of granting and withdrawing access rights to personal data, in particular IT systems, has been developed and implemented.
7. It has been assured that for every person authorized to access the IT system or an element of the IT infrastructure or network a unique ID is assigned that cannot be assigned to anyone else.
8. Periodic access reviews of all users, system accounts, test accounts and accounts are carried out and documented.
9. It has been assured that for every person authorized to access the IT system or an element of the IT infrastructure or network, authorization which takes place, is carried out using secure methods of transmitting the authentication data.
10. It has been assured that password assigned to every person authorized to access the IT system or an element of the IT infrastructure or network is subject to audit procedures and must be changed at predetermined intervals.
11. A standard for secure transmission of passwords has been developed and implemented in case of

the need to provide the IT system user with a temporary password.

12. A standard for creating secure passwords for IT system users has been developed and implemented.

IV. Security of the Service.

1. Elements of the network infrastructure used to process personal data are secured against the loss of accessibility through application and provision of maintenance services provided by producers and distributors.
2. Periodical independent tests of the vulnerability of IT systems that process personal data to threats are carried out.
3. Security gaps are periodically scanned on the platforms and in the networks that process personal data so that general security standards connected specifically with system reinforcement are complied with.
4. As a result of penetration tests, vulnerability scanning and compliance assessment, a corrective program is run on a periodic basis according to a risk-based approach to make effective use of the tests' results.
5. A training program regarding the rules of secure software has been developed and provided.
6. A software security testing program has been developed and provided.
7. The subcontractor and provider selection rules that have been developed guarantee adequate level of technical and organizational security of the services provided and the tasks performed.
8. The sub-processors and other service providers auditing standards and mechanisms have been developed and their implementation has been guaranteed.

V. Change and incident management.

1. A documented change control policy has been put in place which includes requirements for approving, classifying and testing the back-out plan and the division of responsibilities between request, approval and implementation.
2. A standard regarding software production security has been developed and put in place.
3. Procedures for managing and responding to security breach incidents have been put in place to allow reasonable detection, testing, response, mitigation of consequences, and notification of any events that involve a threat to the confidentiality, integrity, and availability of personal data. The response and management procedures are documented, checked and reviewed at least on an annual basis.

VI. Privacy security.

1. A standard regarding the analysis of the risk of violating the basic rights and freedoms of data subjects and the risk of loss of personal data confidentiality, availability and integrity at every product life cycle stage has been developed and put in place.
2. A standard regarding compliance with the privacy protection principle at the software design stage has been developed and put in place (privacy by design).
3. A standard regarding compliance with the privacy protection principle in default settings at the software design stage has been developed and put in place (privacy be default).

B. Technical security measures.

I. Security of personal data processing operations.

1. A minimum scope of technical security measures that needs to be implemented to ensure protection of personal data has been established. Type and scope of the applied additional technical measures for the protection of personal data is established on a case-by-case basis, depending on the identified threats, the required degree of protection and the technical possibilities.
2. The buildings and areas with the rooms used for personal data processing are secured against unauthorized access through application of access control systems, a burglar and attack alarm system, and surveillance by physical security guards, mechanical or code locks.
3. The buildings and areas with the rooms used for personal data processing are secured against fire through application of doors of an increased fire resistance class.
4. The buildings and areas with the rooms used for personal data processing are secured against destruction as a result of fire or flooding trough application of a fire alarm and a burglar or attack alarm system.
5. The buildings and areas with the rooms used for personal data processing are secured to monitor and identify any threats or undesired events through the application of CCTV.

II. Data transmission security.

1. Personal data transferred through teletransmission are secured against loss of confidentiality and integrity using cryptographic data protection measures (data encryption in transit).
2. Personal data transferred through teletransmission are secured against loss of confidentiality through segmentation of ICT networks (network segmentation).
3. Encryption keys used to secure teletransmission of data are stored in a secure place with management of access to them and with the possibility of key recovery.

III. Security of storage devices.

1. Personal data stored in data storage devices at rest is secured against loss of confidentiality and

integrity using cryptographic data protection measures (data encryption at rest).
2. Personal data stored in data storage devices is secured against loss of confidentiality through physical or logical data separation (data separation).
3. Personal data stored in data storage devices is secured against loss of availability and integrity through real-time data copying mechanisms (data replication).
4. Personal data stored in data storage devices is secured against loss of availability and integrity through mechanisms of creating incremental or full data backups at predetermined time intervals (data backup).
5. Personal data stored in data storage devices is secured against loss of availability through mechanisms and procedures for data recovery, data source switching and backup restoration.
6. The data storage devices used for personal data processing are secured against unauthorized access before they are installed in the hardware through access restriction and control using safes.
7. The data storage devices used for personal data processing are secured against loss of data confidentiality through the application of embedded procedures of cryptographic data protection (cryptographic protection of data storage devices).
8. The data storage devices used for personal data processing are secured against loss of availability through the application of systems for automated monitoring of performance, capacity utilization and availability time.
9. The data storage devices used for personal data processing are secured against unauthorized use with the procedures for use and configuration of IT infrastructure elements (configuration management).
10. The data storage devices intended for reuse are secured against data disclosure to any unauthorized person or IT system through the application of secure data deletion methods.
11. The data storage devices used for personal data processing intended for elimination are secured against reuse through permanent and deliberate mechanical destruction.

IV. Data storage security.

1. Personal data stored in databases is secured against loss of integrity through the application of consistency rules in terms of semantics (definition of data type), in terms of entities (definition of basic keys) and in terms of reference (definition of foreign keys).
2. Personal data is secured against loss of accountability through application of solutions that tie specific actions to a specific person or IT system.

V. Security of network infrastructure.

1. Personal data is secured against loss of confidentiality through application of secure access authentication methods for people and IT systems.
2. Personal data is secured against loss of confidentiality and availability through monitoring of correct functioning and use of secure access authentication methods for people and IT systems.
3. Personal data is secured against loss of availability through application of additional, backup and emergency sources of power for the IT infrastructure used to process personal data.
4. Elements of the network infrastructure used for personal data processing (computers, servers, network equipment) are secured against access by unauthorized persons and IT systems through secure access authentication methods.
5. Elements of the network infrastructure used for personal data processing are secured against access by unauthorized persons and IT systems and against loss of availability through monitoring of the validity of the operating system and the installed software.
6. Elements of the network infrastructure used for personal data processing are secured against access by unauthorized persons and IT systems and against loss of availability with use of such software as Firewall, Intrusion Detection Systems, Intrusion Prevention Systems, Anti DDOS.
7. Elements of the network infrastructure used for personal data processing are secured against loss of availability through the application of replication, virtualization and automated scaling procedures.
8. Elements of the network infrastructure used for personal data processing are secured against loss of availability through the application of automatic availability, load and performance monitoring processes.
9. Elements of the network infrastructure used for personal data processing are secured against loss of availability through the application of backup power sources and automatic power source switching procedures.

Annex 3 – List of GetResponse's sub-processors

GetResponse uses the support of its subsidiaries, as well as external sub-contractors to provide the Service. The sub-processors listed below provide services supporting some of the tools of the Service (webinars), hosting and colocation, customer support, incident tracking, troubleshooting, and services concerning identifying and solving problems in the Service.

Name of sub-processor	Corporate location
ArtNet Sp. z o.o.	Poland
ClickMeeting Sp. z o.o.	Poland
OVH	France Canada
TierPoint	USA