PRIVACY AND DATA PROTECTION POLICY

THIS PRIVACY AND DATA PROTECTION POLICY IS AN INTEGRAL PART OF THE TRIGGMINE OÜ TERMS OF USE. ALL DATA SUBJECTS AND OTHER SUBJECTS CONCERNED ARE REQUIRED TO READ THIS PRIVACY POLICY TO UNDERSTAND HOW TRIGGMINE OÜ COLLECTS AND PROCESSES PERSONAL DATA WHILE CONDUCTING ITS ACTIVITIES AND WHAT SECURITY MEASURES ARE BEING APPLIED.

While conducting its activities, Triggmine OÜ (the Company) adheres all conditions and requirements stipulated by the current legislation of Estonia, European legislation, including but not limited to, the GDPR as well as by other international legislative acts concerning data protection.

RECITALS

The General Data Protection Regulation 2016 (GDPR) replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its main purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

In collecting and using of personal data, the Triggmine OÜ is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Triggmine OÜ is taking to ensure that it complies with it.

This Policy applies to all Triggmine OÜ employees/staff, stakeholders and all other subjects that directly or indirectly participate in the personal data processing within Triggmine OÜ activities.

DEFINITIONS

While processing the personal data, the definitions stated herein have the following meaning:

Personal data – any information relating to an identified or identifiable natural person ("individual"/"data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data (sensitive data) – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller (controller) – a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data processor (processor) - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Data subject – any living individual who is the subject of personal data held by the Company, including Users, Subscribers and employees.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyses or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Automated decision-making – is an ability to make decisions by technological means without human involvement.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – is than anyone under the age of 14 years old. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

Company – Triggmine OÜ, legal entity duly registered under the laws of the Republic of Estonia.

Web-site – the web-site http://www.triggmine.com which is owned by the Company.

Clients – individuals or legal entities including officers who act on behalf of such entities, which intend to use the Company's Services, and which collect the personal data of Subscribers.

Subscribers – individuals the personal data of which are being collected and processed by the Clients and might be transferred to the Company with purpose of processing in the interests of the appropriate Client.

Users - individuals who register on the web-site and create an account on the web-site on behalf of himself/herself or representing the interests of the Clients or prospective Clients.

Partners – legal entities the personal data might be transferred to with a purpose of their processing in the interests of the Company. Herewith, such partners can act as Processors as well as Sub-processors, depending on the circumstances.

Software (or "PP") – a computer program developed by the company, provided for use in the form of Internet service, available at www.triggmine.com and additional program code that is installed on the site Processor.

Services – services provided by the Company via using the Software and the main conditions of which are stated on the Website.

Data Protection Authority (DPA) – means an independent public authority which is established by a Member State pursuant to the GDPR. In the contents of this Policy the DPA means an Estonian Data Protection Inspectorate, that is located at the following address: **19 Väike-Ameerika St., 10129 Tallinn. Telephone (from abroad add +372) 627 4135.**

STATEMENT

Triggmine OÜ, registered at the following address: **Estonia pst 5 Kesklinna linnaosa, Tallinn Harju maakond 10143**, is committed to compliance with all relevant EU and Estonian laws in respect of personal data and protect the "rights and freedoms" of individuals while collecting and processing the personal data in accordance with the General Data Protection Regulation (GDPR).

This Privacy and Data Protection Policy (Policy) sets out how we the Company uses, processes and stores the Data Subjects' personal information. The company may get that information from you or from its partners in order to deliver contractual obligations. In other cases, the Company will get that information from you with your permission and consent, or we may receive your personal information from third parties who you have given consent to pass this information on to us.

This Policy describes the main steps the Company makes to be in compliance with the GDPR, herewith, other conditions of compliance along with connected processes and procedures, may be described by other relevant documents, which the Data Subjects and any other stakeholders may find at the appropriate reference links stated herein.

PRINCIPLES OF PROCESSING

While conducting collecting and processing the personal data, the Company adheres the principles provided by the GDPR. The Company's policies and procedures are designed to ensure compliance with the principles.

(a) Lawfulness, fairness and transparency

Lawful – the controller identifies a lawful basis before to process the personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order to process fairly, the controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – any information and communication relating to the processing of the personal data be easily accessible and easy to understand, and that clear and plain language be used;

(b) Purpose limitation
The personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes;

(c) Data minimization
The personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) Accuracy
The personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) Storage limitation
The personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the GDPR Article 89(1) subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject;

(f) Integrity and confidentiality
The personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

PERSONAL DATA THE COMPANY COLLECTS AND PROCESSES

While conducting its activities, the Company collects and processes the following personal data:

1. The personal data of Users. It means that the Company processes the following the Users' personal data: Name; Surname; E-mail, Bank card number.

2. The personal data of the Subscribers. The Company processes the Subscribers' personal data received from the Clients, herewith the scope of personal data is specified by the respective Client solely. That might be the following data: Name; Surname; E-mail, ID, orders, visits, navigation and an information on activities on the Clients' websites.

The company does not collect more personal data than it is needed for the purposes of processing specified herein.

While collecting and processing the personal data of Users, the Company acts as the controller thus, the corresponding range of controller rights and responsibilities arises.

While processing the personal data of the Subscribers, the Company acts as the processor. Therefore, the Company does not have any obligations of the controller under the GDPR, regarding the personal data of Subscribers.

The Company does not collect and/or process any sensitive data within its activities.

THE PURPOSE OF PROCESSING

GDPR requirements

Under the GDPR, there should be specified one or more specific purposes for which the personal data are to be processed. Herewith, it is unlawful to collect and process personal data, not for the purposes defined earlier.

The personal data of Users

The personal data of the Users are being collected and processed for the following purposes:

1. to provide Services specified herein, the Company provides to the Clients, the respective Users act on behalf of and to be in touch with the Users by providing new features announcements and our advices of best practices;

2. to be fast and close to the Users when they need to contact the Company's Support team;

3. to collect statistics and analytics of active marketing campaigns of the Users or the Clients they act on behalf of, using Company's Services;

4. to process your fee for using the Company's Services;

5. to send activation e-mails to the Users during the registration on the Website;

6. to send informational e-mails to the Users and the Clients they act on behalf of.

The personal data of Subscribers

Acting as the processor when processes the personal data of the Subscribers, the Company does not have any obligations to define any purposes of personal data processing.

The purposes of processing of the Subscribers' personal data must be set out by the respective Client who takes on the role of the controller while cooperating with the Company.

Herewith, while providing Services to the Clients, the Company may process the Subscribers' personal data received from the Clients and analyze buying and visit behavior of the Subscribers within Clients web-shops in particular to ensure best efficiency of marketing campaigns of the respective Clients.

THE LAWFULNESS OF PROCESSING

GDPR requirements

Under the article 6 of the GDPR, there are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the GDPR. This Policy has been drawn up to identify the appropriate lawful grounds for the processing and to document it in accordance with the GDPR.

The personal data of Users

The Users' personal data are being collected while the appropriate User is registering on the Website. Herewith, the personal data are being collected via a consent, the providing of which is specified herein.

The Company processes the personal data on the basis of the consent that must be obtained from the User in accordance with the GDPR requirements. Herewith, the consent is to be provided upon to the Consent Request Form the Company provide the appropriate User with.

Along with the Consent Request Form, the Company provides the User with the Privacy Notice, which contains, including but limited to, the precise information concerning the purposes of processing and the information on methods of processing as well as on the period for which such personal data are to be stored.

The consent is considered to be provided to after the User has pressed the "I accept" button on the appropriate Consent Request Form provided by the Company through the Website for each separate purpose of processing of the personal data, as it is stated in such Consent.

By giving the consent the User acknowledges and accepts all terms and conditions specified in the Privacy Notice and Consent Request Form as well as all conditions specified in the current Policy.

Herewith, it worth to clarify that the Privacy Notice is to be provided to the Users within the Website right before the appropriate consent/registering form is filled in.

The Company shall be able to demonstrate that consent was obtained for the processing operation if it is required.

The personal data of Subscribers

Acting as the processor when processes the personal data of the Subscribers, the Company does not have any obligation to establish the lawful grounds for processing. Herewith, the Company is obliged to take all reasonable measures to ensure the lawfulness of its actions.

The lawful grounds for the processing of the Subscribers' personal data are defined by the respective Client within its activities. Herewith, the lawful grounds for processing of the Subscribers' personal data are specified in the appropriate Contract between the Company and the respective Client.

AGE OF THE USERS

GDPR requirements

The processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to

the extent that consent is given or authorized by the holder of parental responsibility over the child. Herewith, the Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

Under the legislation of Estonia, the processing of the personal data of a child shall be lawful where the child is **at least 14 years**.

The personal data of Users

The Company collects the personal data on the basis of consent obtained from the individuals who have reached the age of 14.

When the individual is below the age of 14 years, her/his personal data processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

Registering on the Website and giving the Company the consent, the appropriate User acknowledges that he/she reached the age of 14 and has all rights to provide to the Company the consent to his/her personal data processing. Herewith, the Company is not liable for any consequences if it becomes clear that the User has not reached the age of 14 at the moment of the consent providing.

The personal data of Subscribers

Acting as the processor when processes the personal data of the Subscribers, the Company does not have any obligation to establish the age for the obtaining of the consent. Herewith, the appropriate Client, which transfers the Subscribers' personal data to the Company ensures that all personal data are lawfully obtained from the Subscribers.

WITHDRAWING OF CONSENT

The User is entitled to withdraw the consent at any time he/she wishes. The withdrawal of the consent is considered to be properly made after the User has filled in the appropriate form of withdrawal and sent such filled form to the next e-mail address: support@triggmine.com

The personal data of Users, collected by the Company, are being processed in accordance with the principles stipulated by the GDPR. The Company takes all adequate measures to ensure the compliance with the GDPR requirements while processing the Users' personal data.

While processing the Users' personal data, the automatic decision-making and profiling is not applied by the Company.

The appropriate request for withdrawing of the consent shall be examined within 72 hours since a moment the respective form of withdrawal is received, and the adequate decision will be made by the Company.

THE PERIOD OF STORAGE

GDPR requirements

Article 5 (1) (e) of the GDPR stipulates that the Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

The personal data of Users

The Company processes and stores the Users' personal data during the period that is needed for realization of the processing purposes, specified hereinabove. The period of storage may be longer than the period of processing.

Taking into account the purposes of processing, the period of storage of the Users' personal data (period of storage) is no more than 12 months since the date the data processing consent is duly obtained from the User, taking into account any statutory obligations the Company has to retain the data.

After an expiration of the period of storage, the Company obliged to delete the personal data or ask the User to provide the Company with a new consent if the necessity of processing remains actual for the Company or another purpose of processing appears.

The Company is entitled not to store more and delete the earlier collected Users' personal data of at any time if such personal data are not needed more. Herewith, the Company is obligated to notify the respective User about his/her personal data are deleted.

The Company may keep storing the personal data if a subsequent processing is foreseen by law and is deemed relevant for a purpose which is not compatible with the original purpose of processing stated in this Policy. Herewith, under the incompatible purposes means the purposes concerning archiving in the public interest, scientific, statistical or historical use.

The personal data of Subscribers

Acting as the processor when processes the personal data of the Subscribers, the Company does not have any obligation to establish the period of the personal data storage and processing.

The period of processing and storage is defined by the respective Client within its activities. Herewith, the Company is obliged to process and store the Subscribers' personal data for a period that is specified in the Contract between the Company and the respective Client.

SHARING THE PERSONAL DATA

The personal data of Users

The Company does not sell, trade or transfer your personal data to any legal persons, individuals or Third Parties.

The Company does not share your personal data to any legal persons or individuals, except in the circumstances they are processors or sub-processors of the Company.

The personal data of Subscribers

Acting as the processor when processes the personal data of the Subscribers, the Company acts exclusively under the respective Client instructions and does not specified the scope pf parties the Subscribers' personal data should be transferred to or shared with.

PROCESSORS/SUB-PROCESSORS

GDPR requirements

Whenever a controller uses a processor it needs to have a written Contract in place. The Contract is important so that both controller and processor understand their responsibilities and liabilities.

The personal data of Users

While processing the Users' personal data, the Company engages processors which process the Users' personal data only in accordance with the Company's instructions and within appropriate Contracts concluded between them. In accordance with this Policy, the processors are: Amazon, Mailgun, Intercom, Kissmetrics, Paymentwall.

The Company is responsible for the proper processing of the Users personal data under the GDPR. Herewith, each processor is responsible for the adherence of the GDPR as well as for other legislative actions concerning data protection while processing the Users personal data.

The processors are not entitled to define any additional purposes for the personal data processing.

Regarding purposes specified herein, the Company's processors process the Users' personal data in the following order:
While processing the Users' personal data, the Company engages Amazon as a processor. Herewith, all Users' personal data are transferred onto the Amazon' servers.

The company engages the Mailgun as a processor to send e-mails to the Users while providing Services to the Clients. The Company transfers to Mailgun the e-mails, names and surnames with the purpose of e-mailing.

The Company engages and Kissmetrics, which act as processors for the purposes of collecting statistics and analytics of active marketing campaigns of the Users or the Clients they act behalf on. Herewith, the Company transfers the Users' personal data (e-mails, names and surnames) to such processors.

The Company engages Paymentwall as a processor for the purpose of processing your fee for using the Company's Services

The personal data of Subscribers

Acting as the processor when processes the personal data of the Subscribers, the Company acts exclusively under the respective Client instructions. Herewith, the Company may engage sub-contractors to process the Subscribers' personal data. The Company may use above listed companies as sub-processors while processing the Subscribers' personal data. Herewith, such engaging is specified and agreed by the Company and the respective Client in the Contract between them

DATA SUBJECTS RIGHTS

GDPR requirements

Data subjects, the personal data of which are being processed by the Company have rights the GDPR stipulates to the Data subjects.

1. The data subject's right of access. The Data subjects have a right to know whether their personal data are being processed and 2) if so, access such data with loads of additional stipulations stated in the GDPR Article 15.

2. The data subject's right to rectification. When the personal data the Data subject provides the Company with are not inaccurate then, the respective Data subject is entitled to ask the Company to correct them indeed *(GDPR Article 16).*

3. The right to erasure or right to be forgotten. The Data subjects have a right to obtain from the Company the erasure of the Data subjects' personal data without undue delay and the Company shall have the obligation to erase such personal data without undue delay where the grounds, stated in the *GDPR Article 17 applies.*

4. The data subject right to restriction of processing. The Data subjects have a right to limit processing of their personal data with several exceptions under the scope of the GDPR in particular stated in the GDPR Article 18.

5. The right to be informed. The Company obliged to inform Data subjects what data is being collected, how it's being used, how long it will be kept and whether it will be shared with any third parties. This information must be communicated concisely and in plain language.

6. The right to data portability. The Data subjects are permitted to obtain and reuse their personal data for their own purposes across different services. This right only applies to personal data that Data subjects have provided to the Company by way of the consent.

7. The right to object. The Data subjects can object to the processing of personal data that are being processed by the Company. The Company must stop processing personal data unless they can demonstrate compelling legitimate grounds for the processing that overrides the interests, rights and freedoms of the individual or if the processing is for the establishment or exercise of defense of legal claims.

8. The data subject right not to be subject to a decision based solely on automated processing. Data subjects have a right to object to any automated profiling that is occurring without consent. Herewith, the Data subjects have a right their personal data are to be processed with the human involvement.

The personal data of Users

The Users may use exercise any of the abovementioned rights through clicking on the respective menu and fill in the appropriate form available at the following link: http://triggmine.com/legal/Data-subject-reques-form.pdf

Herewith, the specifics of such exercising are specified in the Data Subject Request Procedure available at the following link: http://triggmine.com/legal/Data-subject-request-procedure.pdf

These are the timescales within which the Users may realize its rights, stated above:

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Herewith, all Users are entitled to lodge a complaint with the Company regarding their personal data are being processed. The specifics of the complaints procedure are specified in a Complaints Procedure available at the following link: http://triggmine.com/legal/Complaints-procedure.pdf

The personal data of Subscribers

Acting as the processor when processes the personal data of the Subscribers, the Company acts exclusively under the respective Client instructions, however, the Company is obliged to help the appropriate Client to provide the Subscribers with their rights under the GDPR.

DATA PROTECTION OFFICER

GDPR requirements

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, the Company does not require a Data Protection Officer to be appointed at the moment of the last review of the current Policy.

SECURITY

GDPR requirements

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

The personal data of Users

The Company is responsible for ensuring that any personal data that Company holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorized by Company to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the internal documents of the Company, which are developed and kept by the Company. The Users' personal data shall be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerized, password protected in line with corporate requirements, and/or
- stored on (removable) computer media which are encrypted.

The Users are entitled to request the Company to clarify what security measures are applied while processing the appropriate Users' personal data.

The personal data of Subscribers

The Company applies the equal security measures both to the Users' personal data and the Subscribers' personal data.

DATA BREACH NOTIFICATION

GDPR requirements

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

There are three different kind of breaches under the GDPR:

- "Confidentiality breach" - where there is an unauthorized or accidental disclosure of, or access to, personal data.
- "Integrity breach" - where there is an unauthorized or accidental alteration of personal data.
- "Availability breach" - where there is an accidental or unauthorized loss of access to, or destruction of, personal data.

The personal data of Users

The Company takes all reasonable steps to minimize the risk of the personal data breach while processing the personal data.

In the case of a personal data breach, the Company shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Supervisory Authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of Users.

The risk assessment the Company has to carry out will have determined whether the risk to the rights and freedoms of the data subjects affected is judged to be sufficiently high to justify notification to them.

Also, in the case of a personal data breach, which is likely to result in a high risk to the rights and freedoms of the Users, the Company shall without undue delay notify the appropriate User the personal data of which were breached.

However, if measures have subsequently been taken to mitigate the high risk to the Users, so that it is no longer likely to happen, then communication to the Users is not required by the GDPR.

The Company documents all personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Supervisory Authority to verify compliance with the GDPR.

Under the GDPR the relevant DPA has the authority to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the GDPR.

The respective processor is obligated without undue delay to notify the Company about the breach of the User personal data while processing such personal data under the Company's instructions.

The Users have a right to apply to the Company or to the appropriate Data Protection Authority about his/her personal data breach if he/she becomes aware of it earlier than the Company.

The personal data of Subscribers

Acting as the processor when processes the personal data of the Subscribers, the Company takes all reasonable efforts to detect all security incidents that can lead to the personal data breach and notify the respective Client about such incident as soon as possible.

DATA TRANSFER

GDPR requirements

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of the GDPR, the conditions laid down in the GDPR Chapter 5 are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in the GDPR Chapter 5 shall be applied in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

The European Commission has the power to determine, on the basis of article 45 of the GDPR whether a country outside the EU offers an adequate level of data protection, whether by its domestic legislation or of the international commitments it has entered into. Under the

appropriate Decision of EU Commission, the personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.

The European Commission has so far recognized **Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework)** as providing adequate protection.

Privacy Shield

If it required to transfer personal data from the EU to an organisation in the United States it should check that the organisation the personal data are transferred to. is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organizations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

The personal data of Users

The Company may transfer the Users' personal data to its processors, specified hereabove and which are registered and located in the USA, therefore, it must be understood that the Company transfers the personal data on the basis of an adequacy decision. Herewith, the Company is obliged to notify the appropriate User that his/her personal data are going to be transferred to the USA.

The personal data are being transferred for the purposes defined herein. Herewith, the Company takes additional steps concerning security and safety in particular, an SSL and AES encryption. While transferring the personal data, the Company acts under the GDPR and internal documents developed in accordance with the GDPR, such as Personal Data Transfer Procedure, which can be available for the respective User at the request.

The Company is applying the equal security measures both to the Users' personal data processing within and beyond the European Union.

In any case, the transfers of personal data outside the European Union is being carefully reviewed by the Company prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR.

The Company has received all proper evidences from its processors they are in compliance both with the Privacy Shield and the GDPR.

The personal data of Subscribers

Acting as the processor when processes the personal data of the Subscribers, the Company may transfer the Subscribers' personal data exclusively under the respective Client instructions. Herewith, if the Client asks the Company to use any third party while personal data processing or the necessity to use such third party arises, the Company may engage Amazon, Mailgun, Intercom, Kissmetrics, Paymentwall as sub-processors.

ADRESSING COMPLIANCE TO THE GDPR

The following actions are undertaken to ensure that the Company complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous;
- All staff involved in handling personal data understand their responsibilities for following good data protection practice;
- Training in data protection has been provided to all staff;
- Rules regarding consent are followed;
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively;
- Regular reviews of procedures involving personal data are carried out;
- Privacy by design is adopted for all new or changed systems and processes;

These actions are reviewed on a regular basis as part of the management process concerned with data protection.

The Company has developed all internal documents to define roles among staff concerning the personal data processing within the Company.

ADDITIONAL CONDITIONS

A current version of this Policy is available to all subjects concerned on the Website at the following link: http://triggmine.com/legal/Privacy-policy.pdf

The Company may revise this Policy from time to time. If the Company makes material changes to this Policy, we will notify you by e-mail or by posting a notice on the website prior to the effective date of the changes. By continuing to access or use the website after those changes become effective, you agree to the revised Policy.