Agreement on Personal Data Processing

This Agreement on Personal Data Processing has been entered into by and between Zone Media OÜ ("Service Provider"), as the Processor, and the undersigned client ("Client"), as the Controller, and it is an Agreement ("Agreement") attached to the Central User Contract and General Terms and Conditions for Services of Zone Media OÜ ("Contract"). In case of any conflict or discrepancy between the Agreement and the Contract, the provisions of this Agreement shall prevail.

Service Provider	**Client**
Zone Media OÜ Reg. no. 10577829 Lõõtsa 5, Tallinn 11415, Republic of Estonia	_____ _____ _____
_____ Ardi Jürgens Member of Management Board	_____ _____ _____

With a view to making the Client's Personal Data available to the Service Provider, the Service Provider hereby agrees to process the Client's Personal Data in accordance with the terms and conditions of this Agreement on Privacy and Personal Data Processing ("Agreement"), whereas the Client and the Service Provider represent that the Service Provider is not aware of whether and which Personal Data the Client will process in the framework of the Services provided by the Service Provider.

1. Definitions

1.1. **"Infrastructure of the Service Provider"** means the premises, network, network equipment, servers and software of the Service Provider which are under the control of the Service Provider, and are used for providing the Service in accordance with the terms and conditions or description of the Service;

1.2. **"Appropriate Technical and Organisational Measures"** mean the processes and procedures which, taking into account the state of the art of technology and the costs of implementation, are used for ensuring the appropriate confidentiality, integrity and availability of the Infrastructure of the Service Provider. These measures shall include at least the measures set out in the **Information Security Principles of Zone Media OÜ,** appended to this Agreement as Annex 1, and other measures that will be additionally agreed upon between the Parties;

1.3. **"Data Controller"** and **"Data Processor"** have the meanings set out in the respective Data Protection Laws;

1.4. **"Data Protection Laws"** are:

(a) In the EU Member States, the General Data Protection Regulation (Regulation (EU) 2016/679) or any other applicable laws of the EU or Member State;
(b) In countries outside the EU – similar or equivalent laws, regulations or rules related to Personal Data;
(c) Enforceable guidelines and codes of conduct issued by a local regulatory authority which is responsible for the management of the application of Data Protection Laws; and/or
(d) Amendments, alterations or supplements that are from time to time made to the documents set out in subclauses (a) to (c) above;

1.5. **"Personal Data Breach"** means, in accordance with the definition set out in the General Data Protection Regulation, a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the personal data transmitted, stored or otherwise processed;

1.6. **"ISO 27001"** means the information security standard ISO 27001:2014 (and the updates that are made to it from time to time) or any information security standard that is equivalent with the requirements of ISO 27001:2014;

1.7. **"Personal Data"** has the meaning set out in the Data Protection Laws;

1.8. **"Client's Personal Data"** are the Personal Data uploaded to the servers of the Service Provider by the Client, created in the servers of the Service Provider upon the use of the Service or uploaded to the server by the users of the application(s) of the Client, which are processed, via the services of the Service Provider, by the Client, by a third party appointed by the Client, or by another processor;

1.9. **"Country not Adhering to Data Protection Conditions"** means a country which does not ensure the adequate level of protection of Personal Data within the meaning of the Data Protection Laws; and

1.10. **"Services"** are the services described in the Contract (and any amendments that are made thereto from time to time), provided by the Service Provider in relation to the processing of the Client's Personal Data.

1.11. The terms used in this Agreement have the same meanings as those set out in the Contract, unless specifically provided otherwise.

2. General Provisions

2.1. The Parties represent that considering the fact that the Service Provider shall only enable the Client to use the Infrastructure of the Service Provider for the storage of data and operating of applications, the Service Provider will not have an overview of the Personal Data processed there or of the types of these Data.

2.2. The Parties represent that this Agreement constitutes a complete and final documented guidance for the processing of the Client's Personal Data. Any other guidance shall be

performed provided only that the Parties enter into a respective written agreement, which may bring along additional fees.

2.3. The Parties represent that the Client shall be the Data Controller and the Service Provider shall be the Data Processor. The Service Provider shall have no rights to the Personal Data processed by the Service Provider on behalf of the Client.

2.4. If the Service Provider or its Subcontractor with whom the Service Provider has entered into a Contract for the Processing of Personal Data on its behalf, processes the Personal Data, the Controller of which is the Client, then the Service Provider:

(a) shall process the Client's Personal Data in accordance with the Data Protection Laws;
(b) shall not do or omit anything which may cause a breach of the obligations deriving from the Data Protection Laws by the Client;
(c) shall process the Client's Personal Data only to the extent and in such manner as is necessary for providing the Services set out in the Agreement and in accordance with the instructions given from time to time by the Client. In case the Service Provider is not certain about the parameters of any instructions given by the Client, the Service Provider shall contact the Client as soon as possible to obtain an explanation or for further instructions for the avoidance of doubt;
(d) shall keep the Client's Personal Data in strict confidence and shall not use or disclose them for any other purpose than for the specific purpose permitted under this Agreement;
(e) shall implement Appropriate Technical and Organisational Measures for protecting the Client's Personal Data against unauthorised or unlawful processing, accidental loss, destruction or damage;
(f) shall, upon the respective request of the Client, quickly return to the Client all the Client's Personal Data that are in its power, possession or under its control, including all copies thereof on any media, unless the retention of copies is required under a law or a contractual obligation; and
(g) shall ensure that all the Client's Personal Data shall always be appropriately protected when in the possession or under the control of the Service Provider.

3. Changing circumstances and amendments to laws

3.1. If the Service Provider:

(a) finds out that the Service Provider is unable, for any reason, to perform the obligations deriving from this Agreement and the Service Provider will not be able to remedy such non-performance; or
(b) becomes aware of any circumstances or amendments to the Data Protection Laws which will probably substantially damage the capability of the Service Provider to perform the obligations deriving from this Agreement;

the Service Provider shall inform the Client accordingly, and thereafter the Client will be entitled to suspend the processing temporarily until the processing will be reorganised in the manner allowing to eliminate the non-conformity. If such reorganising is not possible, the Client will be entitled to terminate the processing of the respective part by the Service Provider.

4. Subcontractors

4.1. The Client will allow the use of subcontractors provided that the Service Provider shall remain fully responsible to the Client for the activities of the subcontractors and for the acts or omissions of the subcontractors in relation to the Personal Data Processing. The Service Provider shall submit a list of the subcontractors upon request.

4.2. The Service Provider shall remain the only contact person of the Client regarding all the issues within the scope of application of this Agreement and shall ensure that its subcontractors shall adhere to the binding requirements of this Agreement in the same way as they are applied to the Service Provider.

4.3. The Service Provider shall ensure that all the subcontractors used by it from time to time in the provision of the Services under this Agreement shall perform the confidentiality obligation on substantially the same (and not less restricting) terms and conditions as the ones set out in this Agreement.

5. Terms of access

5.1. The Service Provider shall ensure that an access to the Personal Data shall be enabled only to:

(a) the appropriately authorised officers, employees, agents and contractors ("Employees of the Service Provider") who need an access to the Personal Data in order to perform the Service Provider's obligations deriving from the Contract and this Agreement; and
(b) the part or parts of the Personal Data that are strictly necessary for the performance of the duties of the Employee of the Service Provider.

5.2. The Service Provider shall ensure that all the Employees of the Service Provider:

(a) shall be informed about the confidential nature of the Personal Data;
(b) shall have passed a training on the storage, protection and handling of the Personal Data; and
(c) shall be informed about their own and the Service Provider's obligations and duties deriving from the Data Protection Laws and this Agreement.

5.3. The Service Provider shall take reasonable steps to ensure the reliability of the employees and subcontractors of the Service Provider who have an access to the Personal Data.

6. Transfer

6.1. The Service Provider shall not transfer the Personal Data to any Country not Adhering to Data Protection Conditions outside the European Economic Area and shall not make the Personal Data available from any Country not Adhering to Data Protection Conditions without a prior written approval of the Client.

6.2. Transfer of the Personal Data or providing an access thereto to a third person located outside the European Economic Area (including the affiliates of the Service Provider) which are not located in a Country not Adhering to Data Protection Conditions, shall be

regulated by a data transfer contract between the Service Provider and the Client which shall contain the standard contractual clauses of the Controller and Processor, as published in the Commission Decision of 5 February 2010 (Decision 2010/87/EU) or any other similar contractual clauses that may from time to time be adopted by the European Commission ('EU Standard Clauses').

7. Notices and incidents and Personal Data Breach

7.1. The Service Provider shall inform the Client immediately, and in any case not later than within twenty-four (24) hours if the Service Provider:

(a) receives an inquiry or request for the conduct of an investigation or audit from an authority related to Personal Data Processing, save in case such disclosure is prohibited to the Service Provider by law;
(b) intends to disclose the Personal Data to any authority;
(c) receives a request from a third party or the Client's employee, the Client or a contractual partner for the disclosure of the Client's Personal Data or of any information related to the processing of the Client's Personal Data; or
(d) ascertains or suspects with good reason that a Personal Data Breach has occurred.

7.2. If necessary, the Service Provider shall provide reasonable assistance to the Client in relation to a claim and/or inquiry, investigation or evaluation of processing initiated by the Client's employee, the Client, a contractor or an appropriate authority.

7.3. In case of a Personal Data Breach, the Service Provider shall implement adequate remedies as soon as possible, including informing the Client about the reasons for the breach, conduct of investigation, and submission of a report and proposal for remedies to the Client.

7.4. The Service Provider and the Client shall fully cooperate in order to develop and implement a response plan to be applied in case of a Personal Data Breach.

7.5. The Service Provider shall provide the following information about a Personal Data Breach (and shall update it upon a reasoned request from the Client):

(a) the supposed date and time of the Personal Data Breach, and the date and time when the Service Provider learned about the Personal Data Breach;
(b) the circumstances related to the Personal Data Breach and any relevant facts regarding the nature and extent of the Personal Data Breach;
(c) the name and contact details of the Data Protection Officer of the Service Provider or of any other appropriate contact person providing additional information;
(d) description of the probable consequences of the Personal Data Breach;
(e) description of the measures taken or proposals for eliminating the Personal Data Breach;
(f) all the details of an investigation initiated in relation to the Personal Data Breach (whether it is the Service Provider's internal investigation or an external investigation (e.g. by a regulatory authority));
(g) the volume and details of the complaints received from individuals in relation to the Personal Data Breach.

7.6. The Service Provider shall notify the Client about any Personal Data Breach before notifying any regulatory authority, and shall provide the Client with a reasonable opportunity to review and supplement the notice. The Client and the Service Provider shall use their best efforts to alleviate the effect of the Personal Data Breach.

7.7. At the request of the Client, the Service Provider shall cooperate in order to adequately notify the affected employees or Clients.

8. Secondary processing

8.1. The Service Provider represents that it:

(a) shall not carry out additional investigation, analysis, profiling or any other processing operation which involves the use of any element of the Personal Data (including aggregate data) or information received from the processing of such Personal Data outside the scope of application of the services; and

(b) shall not transfer any files containing the Personal Data to third parties or their agents for further processing without a prior written consent of the Client.

9. Security requirements

9.1. The Service Provider shall not do or omit anything which would damage or may reasonably be expected to damage the Client's systems or Personal Data.

9.2. Organisation of security

(a) The Service Provider shall appoint an Information Security Officer who shall be responsible for ensuring the good practice of information security in the entire organisation of the Service Provider and in relation to the provision of Services, including the publication of the Information Security Policy.

(b) The Information Security Officer of the Service Provider shall be responsible for the functioning of information security in the entire organisation of the Service Provider.

(c) The Service Provider shall ensure the provision of Services in compliance with the Information Security Policy of the Service Provider.

9.3. Administration of access

(a) The Service Provider shall validate the identity of all the employees of the Service Provider who have access to the Client's system. In case of substantiated need, the Service Provider shall inform the Client about the names of the employees of the Service Provider and their necessary and actual level of access to the Client's Information.

(b) The Service Provider shall ensure that the obligations set out in the previous subclause shall be supported by the internal audit data and alert monitoring which shall enable active ascertaining and investigation of any breaches.

9.4. Physical security

(a) The Service Provider shall protect the Client’s Personal Data against damage deriving from unauthorised physical access and/or loss. This includes control of the physical access, such as protection of buildings against unauthorised access (e.g. using

locks, bolts or equivalent measures for doors and windows that are easily opened), limiting physical access to critical areas only with the authorised employees, external persons who carry out supervision and have been granted the respective access rights, and protection of transmission connections and data media.

9.5. Security inspection

(a) The Service Provider shall allow the Client's employees, authorised representatives and other persons to whom the Client is legally required to provide access or inspection rights, to inspect and evaluate the compliance of the Service Provider with the obligations set out in this Agreement. The inspection may also consist of the transfer of the latest certification or audit results, e.g. ISO 27001 certification audit results and statement of applicability.

(b) The persons carrying out said inspections will be entitled to inspect the measures and procedures for inspecting the security risks of the IT systems of the Service Provider and to interview the employees of the Service Provider in order to evaluate the conformity of the foregoing to the obligations set out in this Agreement.

(c) The Service Provider will be entitled to charge a reasonable fee from the Client for participating in the security inspection if the security inspection is not limited to the issue of any existing documentation or is excessive in the opinion of the Service Provider.

10. Indemnity

10.1. The Service Provider shall be liable for all expenses and damage deriving from the inaccuracy of any representations set out in Annex 1 to this Agreement.

11. Termination

11.1. In the event of termination of the Contract:

(a) The Service Provider shall agree to immediately cease the processing of the Client's Personal Data, and if necessary, send all the Client's Personal Data (including any copies thereof) to the Client to the location indicated by the Client;

(b) The Service Provider shall delete/destruct all the Client's Personal Data in its possession in a manner that shall not enable the recovery of the Client's Personal Data beyond the applicable backup policy or beyond the obligation deriving from law, and shall send the confirmation of the Service Provider regarding the performance thereof to the Client; and

(c) In case the deletion/destruction of the Client's Personal Data by the Service Provider is prohibited by law, the Service Provider shall inform the Client, and the Parties shall agree on a plan of when and how the Client's Personal Data which are in the possession of the Service Provider will be deleted or destructed.

Annex 1: Information Security Principles of Zone Media OÜ

1. General provisions

The mission of Zone is to provide simple, fast and reliable solutions for transmission of and processing of information on the Internet.

Information security has a critical role to play in achieving the mission of our company, and the management and employees of Zone are committed to maintaining the confidentiality, integrity and availability of the information assets of the company and its clients.

For example, in the processing of personal data, we have two equally important roles - depending on the context we can be the **controller** or the **processor** of personal data.

Within the context of the General Personal Data Regulation, our main task is to implement sufficient technical and organisational security measures for our services and infrastructure (hosting space, servers, network equipment, etc) to ensure that the data processed by the clients will be protected against accidental or unlawful deletion, unauthorised access or disclosure.

This information leaflet is to provide you an overview of what to do to ensure the security of the data processed in our infrastructure (including personal data).

It is of utmost importance that you examine this leaflet, as Regulation 2016/679 of the European Parliament and of the Council (the General Data Protection Regulation) sets forth the following:

> If personal data are processed on behalf of the controller, the controller shall use only processors providing sufficient guarantees to implement technical and organisational measures in such manner that the processing will meet the requirements of the Regulation and the protection of the rights of the data subject is ensured therewith.

The controller - it means you. You will have to make sure that we as the processor will protect our organisation, services and infrastructure (hosting space, hardware, software, data communication networks and other resources) in accordance with the requirements of laws and the best practices of the industry. You will naturally also have to know what your duties and responsibilities are upon the processing of personal data.

2. Nature of services

Let us start with the general description of our services.

While using our services, you should remember that we provide a major part of our services as universal could services to our clients. It means that these services are not by default adapted individually to you, but meet the general demands of the market. Individual agreements and adaptions are still possible.

As a cloud service provider, we have no control over the data that you upload to our infrastructure or process therein. It means that we do not know by default whether out services are used for the processing of personal data, which personal data are being processed and whether

such processing is lawful. If necessary, you yourself will have to evaluate the effect of data processing and its conformity to applicable laws.

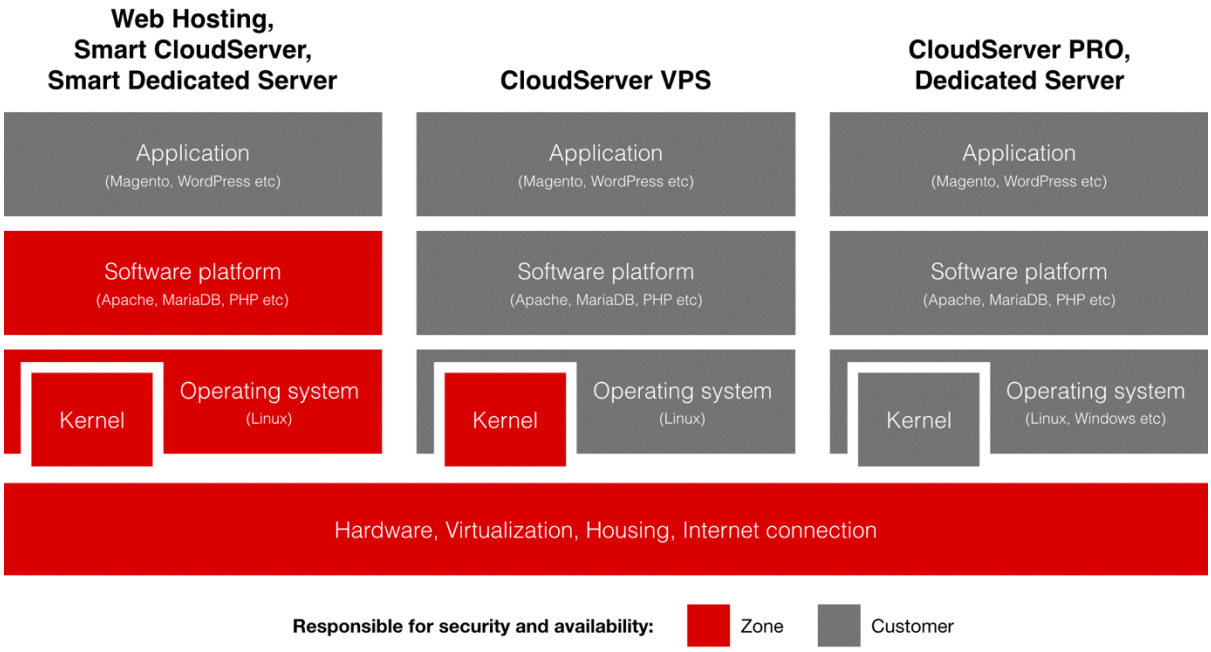
3. Service classes

The majority of the services offered by Zone are classified as cloud services. They are based on the following main cloud service models:

- 'Software as a Service' (SaaS) delivers the ready-to-use application to the client;
- 'Platform as a Service' (PaaS) provides conditions necessary for managing an application;
- 'Infrastructure as a Service' (IaaS) offers virtual servers to the client for creating one's own platform.

The scope of the duties of Zone and of the client vary within the framework of these models in accordance with the chosen service. We have also described it in the leaflet of our every service under the section "Division of responsibility".

The following drawing given a general overview:



The e-mail, DNS and ZoneCloud included in the virtual server service are SaaS services and the responsibility of Zone extends also to the application layer.

It is important to remember that the security of access data, applications and transport of data is almost always in the sphere of responsibility of the client by default.

4. Service delivery models

Three service delivery models are in use:

- Joint use;
- Individual use;

- Hybrid use.

Joint use means that several organisations share the same servers. Services such as the Virtual Server, Cloud Server VPS, Cloud Server Pro and Smart Cloud Server are based on joint use. These services cost less, but they involve also greater risks than individual use - the additional risks are mainly connected with the other users of the service.

For example, in case of joint use there is a possibility that a client may with excessive use of resources negatively affect the availability of the websites of other clients. Zone has a long experience in offering services based on joint use, and the means for mitigating such risk are already included in our software platform, but it is not possible to eliminate the risks relating to availability of resources within 100% in the jointly used environment.

In case of **individual use**, servers are only at the disposal of one client. Individual use is applied in case of the Private Server and partially also the Smart Private Server services, whereby a client receives guaranteed private server resources to its use. In case of individual use, the client does not share the server resources with other clients which will substantially mitigate the risks related to the availability of the service and confidentiality of data. In addition, the individual use enables to implement client-based information security measures to the server(s) as necessary.

The main advantage of individual use is that in case of a potential incident, the restoration of the service to the given client shall be a priority. In case of joint use, the interests of the majority of clients shall be of main importance. The minor disadvantage of the individual use is its higher price.

In case of **hybrid use,** different models may be used for different components of the service. The hybrid model is applied by default to the Smart Private Server service, where the server servicing web applications and database are dedicated only to one client, but the e-mail and DNS services share resources with other clients. In case of special solutions, this division may naturally vary – we will also be able to offer private e-mail servers, etc upon request.

5. Information security at Zone

5.1. Information security process and organisation

It is of primary importance that the organisation shall be devoted to information security. For this purpose, our management has established the Information Security Policy which is implemented all over our company – adherence to the established principles is expected from the managers, employees and also from the contractors of Zone, as they participate in the operations of our company. The up-to-dateness of the policy is assessed at least once a year.

The Information Security Officer is responsible for the preparation, supplementing and implementation of the Information Security Policy.

The Information Security Officer is supported in his work by a broad-based information security team and the Data Protection Officer. All the structural units and employees are naturally engaged in the information security process.

We have developed our **Information Security Policy** in accordance with the standard **ISO/IEC 27001:2014** and our goal for the future is to reinforce our conformity to the standard by undergoing also the official certification process.

Zone shall administer **information security risks** based on the recommendations of the standard **ISO/IEC 27005:2014** and shall use the qualitative asset-based risk weighting methods.

5.2. Security level of the client's information assets

The client is the responsible owner of the client's information assets (files, databases, e-mails, etc) stored and processed in the IT systems of Zone.

The security level of the client's information assets in our internal systems is 'confidential' which is defined as follows: the use of information is allowed only for certain specific groups of users, access to information is permitted in case of legitimate interest of the person seeking access (e.g. if it is necessary for performance of work duties).

The internally applicable security level of Zone is not automatically transferred outside the company. The client has to store, process and transfer his or her information in the IT systems of Zone in accordance with the security levels given by the Client to his or her own information assets, as well as weighted risks, and organise implementation of security measures accordingly.

We never sell any data uploaded to the infrastructure of Zone, uploaded by the client's users or created in the server in the course of the use of the service by the client to anyone, and we shall not use such data without the client's permission in our own direct economic interests. Zone shall process such data only to the extent required for providing its services or user support related thereto.

5.3. Personal data protection at Zone

In order to carry out supervision over personal data protection, we have created the position of a Data Protection Officer, and the person holding this position has undergone also the training programme recognised by the Data Protection Inspectorate.

We maintain records of the processed personal data as well as of the effect of processing on such data.

Further information on personal data processing is available in the **Privacy Policy of Zone Media OÜ**.

5.4. Location of data

We provide our services in physically safe conditions. The data centres used by Zone are located in the territory of the European Union.

For the purpose of hedging information security, durability and business risks and for offering unique opportunities to our clients, our infrastructure is distributed among 5 data centres, 4 whereof are located in Tallinn, Estonia, and 1 is located in Amsterdam, Holland. In infrastructure hosting, Zone co-operates with the acknowledged partners such as Equinix, Linxtelecom, Telia and Elisa.

The data centres used by Zone are located in the buildings constructed or adapted specially for the hosting of information and communication technology equipment and are separated from public space. The equipment is located in premises separated by security fence or in locked equipment cabinets. Access is limited with the persons who have a need for access deriving from their work duties.

Data centres are equipped with security cameras and alarm systems, and a log is maintained regarding entry to the centres. The centres use an automated fire alarm system and automated gas fire extinguishing system.

In order to maintain the temperature and relative air humidity at the level suitable for servers and data communication equipment, all the data centres have cooling equipment and systems.

In order to ensure more reliable power supply, all the equipment of Zone is connected to uninterruptible power supply (UPS) and the buildings have power generators.

In order to ensure availability, all the data centres have redundancy of equipment and technical systems.

The areas where the buildings used by Zone are located are not exposed to any significant risks related to weather or local geology, and no damage has been previously caused to the data centres by these circumstances.

5.5. Data communication

In order to mitigate the risks related to information security, durability and business and to provide unique opportunities to its clients, Zone co-operates with several reliable telecommunication companies. The data communication partners of Zone are Cogent Communications, Level3 Communications, Linxtelecom, Telia and Elisa.

In Estonia, Zone uses parallelly three and in Holland we use two Internet transit connections – the redundancy of connections ensures that the clients have connectivity even during a single connection failure or maintenance work.

Zone has established a unique private regional network between Estonian hosting centres with the purpose of additional management of risks to the availability of services deriving from external conditions. The data centres providing server services are connected to two other centres at the same time - the resulting network setup enables to maintain connectivity at the centre even during a failure or maintenance of one connection.

In addition, Zone is connected with many telecommunications companies and companies providing Internet services in Estonia by two major Internet exchange points of Estonia – TLLIX and RTIX.

Zone will make sure that in normal circumstances the transmission connections would be underutilised and additional resources would be readily available as necessary.

In order to manage specific risks deriving from denial of service attacks, Zone has equipped its Internet connections with special equipment mitigating the negative impact of attacks.

5.6. Backup of data

Zone shall make backup copies of servers related to the services administered by Zone, based on the following rules:

- a backup copy of the files, SQL databases and mailboxes in a web server shall be made at least once a day;
- a backup copy shall be usable for restoring any backed-up data for at least 14 days after the moment when the backup copy was made;
- backup copies shall be made, as necessary, before major software updates or modifications which may endanger the integrity of data.

We store backup copies of the servers used for providing the services administered by Zone separately from the production environment.

In case of services based on individual use, it is possible to adapt the backup policy to the client's needs.

As a client, you will have to take into account that the time of restoring of data depends directly on the nature and volume of data, and in case of joint use, it is also affected by other clients using the same resource.

5.7. Monitoring

Zone shall monitor the work of the servers providing the services 24 hours a day and 7 days a week.

Among other things, Zone monitors any references to the compromising of the platform or the client's services, including the start of unknown processes, opening of unexpected network ports, activity of users, sending of spam, etc.

Active monitoring takes place from 08.30-17.30 on business days. In case of active monitoring the employees of Zone Media monitor the output of the monitoring system in real time, and in addition, the monitoring system informs the technicians of Zone via mobile communication network. Incidents are responded to without delay.

Passive monitoring takes place from 17.30-08.30 on business days and 24 hours during weekends. In case of passive monitoring, the monitoring system informs Zone's technician on call about any problems via mobile communication network. The technician on call shall respond to incidents without delay.

5.8. Client support

The working hours of Zone's telephone support and e-mail support is from 09.00 – 17.00 on business days (time zone EET/EEST).

The client support telephone number is: +372 **688 6886**
The client support e-mail address is: info@zone.ee

Should you have any questions regarding personal data processing, you may contact directly the Data Protection Officer of Zone at the address dataprotection@zone.ee.

The current update of the service platform of Zone is available on the website http://status.zone.eu.

E-mails sent outside the working hours are handled by the team on call which shall organise response to any critical incidents.

The 24/7 helpline is available to the clients of services based on individual use, as necessary, which is meant for notification of critical incidents.

5.9. Processors engaged by Zone

We may engage processors in the processing of a client's data.

We do it only if we are sufficiently certain that they implement appropriate technical and organisational measures in such manner that the processing of data is in compliance with the requirements set out by law.

We publish the list of significant processors engaged in the processing of clients' data on our website (https://www.zone.ee).