GDPR Annex

personal data processing by DAZOOT SOFTWARE SRL according to GDPR directive

(Personal Data Processing Agreement between Data Controller and Data Processor - Newsman.ro)

This Annex provides specific rules regarding the processing of personal data, sent by the Beneficiary, as Data Controller, by DAZOOT SOFTWARE SRL, as Data Processor, in accordance with the Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as "GDPR"), as well as any subsequent national legislation on personal data protection.

Art. 1. In this annex, the terms used shall be interpreted in accordance with the GDPR and, where applicable, they shall have the definitions stipulated by art. 4 of the GDPR.

Art. 2. The purpose of personal data processing is the processing by the Data processor, of the personal data sent by the Data Controller for the purpose of providing the services stipulated in the main software service contract.

Art. 3. The personal data provided by the Data Controller, which are processed under this Agreement are the following:

3.1. First name, Last Name, E-mail, Telephone Number - if applicable - as well as any additional data uploaded by the Data Controller directly or indirectly;

3.2. Data and information directly related to the sent emails or follow up actions such as the list of open newsletters or links accessed (including the time stamping of these actions), actions in email (e.g. unsubscription), IP address from which the actions originated, or - if the customer integrates the JS retargeting code provided by the Data Processor - the pages visited on the Data Controller's site.

Art. 4. The categories of data subjects are subscribers and / or customers of the Data Controller.

Art. 5. Under this agreement, the Data Controller gives the following instructions to the Data Processor:

5.1. Collect and process the personal data received from the Data Controller directly (via upload to Data Processors' platform) or indirectly (through a subscription form of the Data Controller). The related personal data are those ones specified in Article 3.1.

5.2. To send messages via email (newsletter or transactional emails) on behalf of the Data Controller including their personalization, with the content, sending time and subscriber base established by the Data Controller;

5.3. To collect and process data and information directly related to sent emails or follow-up actions, such as those specified in Article 3.2.;

5.4. To send messages via SMS with content, sending time and subscriber base established by the Data Controller if this service is included in the main contract;

5.5. Any other written instruction - electronically or on paper - by the Data Controller related to the activities performed under the software services contract, and that Data Processor does not consider to be contrary to the GDPR.

Art. 6. The duration of the processing of personal data is the same as the duration of the main service contract for the provision of software.

Art. 7. The type and the purpose of personal data processing are those one established by the Data Controller under the main contract and namely, providing services for sending messages via e-mail or SMS, and related services for the analysis and processing of information related to these messages.

Art. 8. In the event that the processing of the Data Controller's data or certain parts of it is carried out by the Data Processor through other persons, called Sub-Processors, it must comply with the following principles:

8.1. Under this Article, the Data Controller understands to authorize the Data Processor to process its data through the following Sub-Processors for the following activities:

- Hetzner AG (Germany) - for server hosting;
- TOP Level Hosting (Romania) - for hosting SMTP servers (data on TLH servers are only in transit - they are not stored);
- LiveShells SRL (Romania) - for hosting SMTP servers (data on NSHost servers are only in transit - they are not stored);
- DA International group Ltd. (Bulgaria) - for hosting SMTP servers (data on AlphaVPS servers are only in transit - they are not stored);
- Village Media SRL (Romania) - for configuring special SMTP servers;
- ANY MEDIA DEVELOPMENT SRL (Romania) - for sending SMS.

8.2. For future Sub-Processors, the Data Processor receives a general authorization to subcontract with any other EU, EEA provider or country with an appropriate level of protection recognized by the EC Decision, which is required for certain parts of the data processing under this contract, offering an appropriate security level, at least at the same level of this contract. This authorization includes the obligation to inform the Data Controller through a message via the account of the Data Processor’s website or via email. The Data Controller has the opportunity to raise objections within 2 working days.

Art. 9. Rights and Obligations of the Data Controller

9.1. The right to receive information or to verify, directly or by mandated auditor, in order to find out how the Data Processor implements appropriate technical and organizational measures so that the processing complies with the requirements of the GDPR; verification will take place on the basis of a prior written notification submitted at least 14 working days before verification date;

9.2. The right to receive assistance from Data Processors' side, especially for fulfilling its obligation to respond to the requests of the individuals (data subjects) concerned about the exercise of their rights under GDPR;

9.3. The right to object to other Sub-Processors according to Article 8.2;

9.4. To comply with its obligations under the GDPR as Data Controller regarding personal data collected or processed by the Data Processor, on his behalf;

9.5. In particular, to be solely responsible for obtaining the consent of the data subjects (or to use another legal basis) for the processing of personal data which is the subject of this Agreement, including when the Data Processor is authorized by this Agreement to collect personal data on behalf of the Data Controller;

9.6. In all cases where the Data Controller is the one who has to perform an obligation, such as informing the data subject about personal data breach, the Data Processor may not be held responsible for the Data Controller's inactions within the scope of that obligation,

Art. 10. Rights and Obligations of the Data Processor:

10.1. The obligation to inform the Data Controller, within maximum 10 days if, in the Data Processor's view, an instruction violates the GDPR and / or any other legal provision regarding the processing of personal data;

10.2. The obligation to ensure the security of personal data processed on behalf of the Data Controller in accordance with Article 32 of the GDPR and Article 11 of this Annex;

10.3. The obligation to inform the Data Controller without undue delay within 48 hours of a security breach regarding the personal data of the Data Controller during the processing performed by the Data Processor;

10.4. The obligation to assist the Data Controller with all necessary information to notify, if necessary, the Competent Authority about a data breach, but without substituting the Data Controller for its notification obligation

10.5. The obligation to assist the Data Controller to ensure compliance with the obligations under Articles 32-36 of the GDPR;

10.6. The obligation to assist the Data Controller in resolving the requests of the data subjects or to transmit to the Data Controller any request received from the data subjects regarding the personal data that were collected and processed by the Data Processor, within a maximum of 5 calendar days from its receipt. This assistance does not apply if the Data Controller already has the technical means provided by the Data Processor to resolve the request of the data subject (e.g. unsubscription of the data subject);

10.7. The obligation not to transmit personal data and / or confidential information, which may be personal, which he became aware of during the execution of the contract;

10.8. The obligation to provide training to authorized personnel to process personal data, with regard to the confidentiality of such data;

10.9. The obligation to include confidentiality obligations to employees and sub-processors;

10.10. The right to disclose certain personal data at the request of an authority, public institution or court or other third party authorized under the law, by virtue of a legal obligation or other condition prescribed by law;

10.11. The right to recruit sub-processors in accordance with art. 8.1 and 8.2, or for whom the Data Controller has given his/her approval;

10.12. The right to cover the costs incurred in assuring the Data Controller's assistance in the GDPR cases, if they exceed the monthly cost of services rendered by the Data Processor;

10.13. The right to use anonymized statistical information as a result of the activities performed under this contract or for its entire activity;

10.14. The Data Processor may not establish purposes or means of processing personal data, these being determined solely by the Data Controller.

Art. 11. The Data Processor has established the internal application of the following organizational and technical security measures for the security of personal data, taking into account the type of activity performed:

- Regular personnel training (internal security policy);
- Office access with key and / or Nuki Smart Lock;
- Workstations with encrypted hard drives;
- Storage of personal data exclusively in the data center (nothing is stored in the office);
- Access backend SSL (secure) just using 2-step authentication;
- Employee access to backend is limited (they do not see the personal data loaded by the Data Controller);
- Server access via VPN + SSH Agent (RSA 2048 bit keys, stored exclusively on encrypted hard drives);
- Secure servers (updates daily + running IDS - Intrusion Detection System);
- Servers with restrictive firewall.

Newsman application security:

- Access only via SSL (secure) protocol;
- 2-step authentication (login);
- Option sub accounts (accounts with restricted access to the application, e.g. only read or only editor, without the option to download the database);
- Brute Force Protection (IP lock after a few failed attempts);
- Strong password (minimum 10 characters, one uppercase letter, one lowercase letter, one number and special characters/symbols);
- Protection session hijacking (session capture);
- CSRF / XSS protection;
- High Security Mode (reintroduction of 2-step authentication code) required to access sensitive areas of application (e.g.: viewing email addresses or editing a profile or downloading databases) - code expires in 4 hours after activation;

- Notifications download links that expire in 4 hours, extensive logging downloads;
- New IP / country logon notifications (if 2-step authentication is not enabled);
- Password change or profile data update notifications (unless 2-step authentication is activated);
- Monthly scan of application vulnerabilities.

These measures are centralized within the Internal Security Policy, which can be made available upon request.

Art. 12. The Data Controller agrees to exempt the Data Processor of any liability for damages that may arise from:

12.1. failure to comply with the contract due to events that exceed any liability of the Data Processor;

12.2. compliance with the Data Controller's instructions or non-compliance with Data Controller's instructions previously warranted by a notification of its unlawfulness;

12.3. the lack or violation of the consent of the data subjects or the use of a wrong legal basis by the Data Controller; failure to comply with the contract due to some Data Controller's actions.

Art. 13. This Annex shall enter into force on May 25, 2018.

Provider (Data Processor) SC Dazoot Software SRL	Beneficiary/Client (Data Controller) ……..
Managing Partner, Cătălin Constantin	Managing Partner, ……..