Personal Data Processing Agreement

(hereinafter referred to as "the Agreement")

CALAMARI Sp. z o.o. Sp. k. ul. Chmielna 2/31, 00-020 Warszawa, POLAND, hereinafter referred to as the "**Processor**",

and

the Client (Recipient) hereinafter referred to as the **"Data Controller"** / **"DC"**

§ 1

Entrusting the processing of personal data

1. The Data Controller entrusts to the Processor in the mode of article 28 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/4/2016 on the protection of individuals with regard to the processing of personal data and on the free flow of such data and repealing the Directive 95/46/EC (Official Journal of the UE L No. 119, p. 1, as amended), hereinafter referred to as the "GDPR", personal data for processing, on terms and in accordance with the purpose set out in this Agreement.
2. The DC declares and ensures that it has a legal basis for data processing, and entrusting the Processor with data for processing will not violate the rights and liberties of entities of such data, as well as legal provisions (in particular the GDPR).
3. The Processor undertakes to process the personal data entrusted to it only at the request of the DC, in accordance with this Agreement, the GDPR, and generally applicable laws protecting the rights of data subjects.
4. The Processor declares that he applies technical and organisational security measures in order to appropriately protect personal data against destruction, loss, modification, unauthorised disclosure or unauthorised access. The list of applied security measures shall be presented in a reply message, at the Controller's request sent to the following e-mail address: dpo@calamari.io

§ 2

The scope and purpose of data processing

1. The purpose of personal data processing is to provide the DC with a service supporting staff management processes, in particular, time records and absence management, due to the cooperation between the DC and the Processor based on the current Calamari Terms of Use and other contracts concluded by the Parties.
2. The Processor, as a provider of the Calamari web application, shall process entrusted, regular data and sensitive data of adults who cooperate with the Controller.
3. The data entrusted for processing is such data as: name and surname, email address, date of employment, start and end of work, breaks at work, information on holidays, information on sick leaves, work schedule, date and time of absence from work, reasons for absence at work, GPS location (in the case when the Controller enables the GPS location tracking), IP addresses (in

the case when the Controller enables the IP address tracking) and identifiers used in computer systems.

4. The Processor may process personal data only for the purpose of providing the service used by the DC, as well as performing other processing operations of personal data stipulated in this Agreement, not directly covered by the subject of the services but supporting the use of the Calamari Application in accordance with the arrangements between the Parties.
5. If, in connection with the use of the services of the Processor, after the Processor's approval, the DC enters other personal data than those listed in sections 3 and 4 above, he also entrusts them for processing on the terms of this Agreement.
6. The Processor, within the goal of processing the personal data entrusted, is entitled to perform an operation or set of operations which is performed on personal data or on sets of personal data such as recording, organisation, structuring, storage, browsing, alignment or combination, restriction, and destruction.

§ 3
The manner of performance of the Agreement in terms of personal data processing

1. The Processor undertakes to process the personal data entrusted to him in a safe manner by applying appropriate technical and organizational measures ensuring an adequate level of security corresponding to the risk related to the processing of personal data, referred to in Article 32 the GDPR.
2. The Processor undertakes to exercise due diligence in the processing of entrusted personal data.
3. The Processor undertakes to grant written authorizations to processing of personal data to all persons who will process the entrusted data in order to perform this Agreement.
4. The Processor undertakes to ensure the confidentiality of processed data by persons who are authorised to the processing of personal data for the purpose of implementing this Agreement, both during the cooperation and after its termination.
5. The Processor undertakes to make personal data accessible only to persons who are suitably skilled and experienced and have the necessary knowledge of personal data protection adequate to the obligations related to the processing of personal data and have been authorized by the Processor to process personal data.
6. After the Agreement termination or completing the service, the Processor shall allow the DC to download the data and will immediately delete the Data Controller's account, and delete all existing copies of the data unless EU law or the law of a Member State requires the storage of personal data.
7. After identifying a breach of personal data protection, the Processor reports it to the Controller without undue delay. The infringement notification shall contain:

a) a description of the nature of the personal data breach, including where possible the categories and approximate number of data subjects, as well as the category and approximate number of entries of personal data affected by the breach;

b) a description of possible consequences of a breach of personal data protection;

c) a description of the measures used or proposed by the Processor to remedy the infringement of personal data protection, including, where appropriate, measures to minimise its potential adverse effects;

d) contact details of the person responsible for providing information regarding the breach.

8. If possible, the Processor assists the Controller in the necessary extent to fulfil the obligation to respond to requests of the data subject, fulfill the obligations related to ensuring adequate data security of personal data, obligation to report violations of personal data protection or obligation to assess the impact for data protection (resulting from Articles 32-36 of the GDPR).
9. If the data subject transfers the request directly to the Processor, the Processor shall immediately inform the Controller about the submitted request. The Controller is solely responsible for preparing a response to the request of the data subject.

§ 4
Control rights / Audits

1. The Data Controller, in accordance with Article 28 section 3(h) GDPR, has the right to control whether the means used by the Processor in processing and securing entrusted personal data meet the provisions hereof.
2. The right of control can be executed remotely, via the e-mail address: dpo@calamari.io by directing a list of control questions or requests to which the Processor undertakes to respond in a return message.
3. The Data Controller may exercise the right of control during the Processor's working hours and with his forewarning of at least 30 days, along with an indication of the list of persons involved in conducting the Audit on the DC side.
4. Each time before the audit, the Controller will submit a framework plan of control activities to the Processor for verification and acceptance.
5. Audits are carried out at the expense of the Data Controller.
6. In the case of unreasonable, overly-repeated audits of a wide scope or taking place outside the dates resulting from the audit schedule, the Processor may introduce a fee for auditing in the amount resulting from the administrative costs incurred.
7. The Processor undertakes to remedy the shortcomings found during the inspection by the deadline specified by the Controller, not longer than 30 days.
8. The Processor shall immediately inform the DC, if in his opinion, the instruction given to him constitutes a violation of the GDPR or other generally applicable provisions regulating the protection of personal data.

9. The Processor provides the Controller with all information necessary to demonstrate compliance with the obligations set out in Article 28 the GDPR.

§ 5
Sub-processing

1. The Processor may entrust personal data covered by this Agreement for further processing to subcontractors and providers only for the purpose of providing the services referred to in the Calamari Terms of Use and other agreements that the Parties have concluded.
2. The Processor entrusts personal data covered by this Agreement for further processing to external entities within the European Economic Area. Data is entrusted only for the purpose and scope of performance of this Agreement, for which the Processor receives the Controller's consent.
3. The list of entities sub-contracted for data processing is available at the request of the DA, directed to the following e-mail address: dpo@calamari.io.
4. The Processor, by e-mail, informs the Controller about any intended changes regarding the addition or replacement of other processors than these listed on the list of entities. The Controller has the opportunity to object to such changes within 7 days.
5. The Processor has a personal data processing Agreement to entrust the processing of personal data with the entities indicated on the list of entities sub-contracted to the processing of personal data or these entities provide sufficient guarantees of appropriate technical and organisational measures to ensure that the processing meets the requirements of the GDPR.

§ 6
Responsibility of the Processor

1. In the event of a breach of the provisions of the Agreement or applicable legal provisions for reasons attributable to the Processor, as a result of which the Controller will be obliged to pay compensation or will be punished - the Processor is liable only if he has not fulfilled the obligations that the GDPR directly imposes on the processing entities, or when the Processor operated outside the lawful Controller's instructions or contrary to these instructions.

§ 7
Confidentiality

1. The Processor undertakes to keep confidential all information, data, materials, documents and personal data received from the Controller and from the persons cooperating with him and the data obtained in any other way, deliberate or accidental, in verbal, written or electronic form ("confidential data").
2. The Processor declares that in connection with the obligation to keep confidential data in secrecy, they will not be used, disclosed or made available without the written consent of the Data Controller for a purpose other than the performance of the Agreement, unless the necessity to disclose the information possessed results from the applicable provisions of law or the Agreement.

3. The Parties undertake to make every effort to ensure that the means of communication used to receive, transmit and store confidential data guarantee securing confidential data, in particular personal data entrusted to processing, against unauthorised access to their content by third parties.

§ 8
Duration of processing

1. This Agreement is in effect for the duration of the services provided by the Processor until the data is deleted.
2. The Agreement is terminated upon the completion of the use of the services provided by the Processor.
3. After completing the provision of services related to the processing of the Data for the DC, the Processor allows downloading the data and immediately deletes the DC account and erases all existing copies of the data - no later than 90 days after the end of service, unless legally binding provisions of law require storage of personal data.

§ 9
Final provisions

1. This Agreement supersedes all previous contracts, arrangements and agreements regarding the entrusting of personal data.
2. In the event of a conflict between the provisions of this Agreement and the Regulations and other agreements concluded by the Parties, the provisions of this Agreement shall prevail.
3. All changes to the Processing Agreement will be published on the website as an attachment to the Regulations. In addition, the DC will be notified of changes 21 days prior to their entry into force, via e-mail address or via the service interface.

On behalf of the Client
Company: ________________
Name and surname: ______________
Position: _________________
Signature: ______________________

On behalf of the Calamari
Company: **Calamari sp. z o.o. sp. k.**
Name and surname: **Kamil Wojewoda**
Position: **Member of the Board**
Signature: Kamil Wojewoda

PODPIS ZAUFANY
KAMIL
WOJEWODA
06.12.2022 12:14:13 [GMT+1]
Dokument podpisany elektronicznie
podpisem zaufanym