Data Processing Agreement

This Calamari Data Processing Agreement (“DPA”) reflects the parties’ agreement with respect to the terms governing the processing of personal data under the Calamari Terms of Use (the “Agreement”). This DPA is an amendment to the Agreement and is effective upon its incorporation into the Agreement. Upon its incorporation into the Agreement, the DPA will form a part of the Agreement.

If you accept this DPA on behalf of Client, you warrant that:

(a) you have full legal authority to bind Client to this DPA;
(b) you have read and understand this DPA;
(c) you agree, on behalf of Client, to this DPA;
(d) you also warrant that the information submitted in signing up is correct and accurate to the best of your knowledge.

The parties acknowledge and agree that in relation to any personal data in Client’s Company Account:

(a) Client will be the Controller of the personal data; and
(b) Calamari will be the Processor of such personal data.

Each party will comply with the obligations applicable to it under the Data Protection Laws with respect to the processing of personal data.

This DPA includes:

1. Personal data processing specification
2. Technical and organizational security measures
3. Sub-processors list

Personal data processing specification

Definitions

"**Account**" ("Client's Company Account", or "Company Account") means collectively all the information, payment information and credentials, Personal Data added and used by Client in Calamari Services;

"**Agreement**" ("End User Licence Agreement", or "EULA", or "Terms of Use") means binding agreement that shall come into effect between Client and Calamari;

"**Calamari**" ("Calamari",or "Vendor") means CHROBRUS Hubert Lisek (Tax ID, NIP: PL 7182035805), registered office: ul. Stanisława Tońskiego 31; 18-414 Nowogród, Poland which develops, manages and provides Calamari Services;

"**Client**" ("Customer", or "You", or "Yours") means any organisation which chooses to implement Calamari within their organisation;

"**Controller**" means 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;

"**Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 and the Polish Act of 29 August 1997 on Personal Data Protection (Journal of Laws of 2002 No. 101 item 926, as amended);

"**Data Protection Officer**" ("DPO") is as defined in the EU General Data Protection Regulation 2016/679, Articles 37-39.

"**Data Subject**" means an individual who is the subject of Personal Data;

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

"**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, 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;

"**Personal Data Breach**" means a breach of Calamari security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data in systems managed by Calamari. Personal Data Breach will not include unsuccessful

attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems;

"**Processor**" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of Controller;

"**Sensitive Personal Data**" means any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data, data concerning health, data concerning sex life or sexual orientation and data concerning the commission or alleged commission of any offence;

"**Sub-processor(s)**" means third parties authorised under this Data Processing Agreement to have logical access to and process Personal Data in order to provide parts of Calamari Services and any related technical support;

"**Service(s)**" means the online human resource services developed, operated, and maintained by Calamari, or ancillary online or offline products and services provided to Client by Calamari, to which Client is being granted access;

"**User(s)**" ("Client's Users") means Client's employees, representatives, consultants, contractors or agents who are authorised to use the Service and have been supplied user identifications and passwords by Client (or by Calamari at Client's request);

Any phrase introduced by the terms "including", "include" or any similar expression will be construed as illustrative and will not limit the sense of the words preceding those terms. Any examples in this DPA are illustrative and not the sole examples of a particular concept.

Application of this DPA

This DPA will apply:

(a) if Client clicked to accept this DPA; or
(b) if the Agreement incorporates this DPA by reference.

The effective date for this DPA will be, as applicable:

(a) 25 May 2018, if Client clicked to accept or the parties otherwise agreed to this DPA before or on such date; or
(b) the date on which Client clicked to accept or the parties otherwise agreed to this DPA, if such date is after 25 May 2018;
(c) the date on which Client clicked to accept or the parties otherwise agreed to Calamari Terms of Use which incorporate this DPA by reference and such date is after 25 May 2018.

Details of the Processing

(a) Categories of Data Subjects. Controller's employees, representatives, consultants, contractors or agents. All individuals whose Personal Data have been stored in Calamari Services by Controller (or by Calamari at Controller's request).

(b) Types of Personal Data. Processor may process the following:

(i) all data (including any potentially Sensitive Personal Data) which has been stored in Calamari Services by Controller, Users or by Processor at Controller's request which may include:

(1) contact data, dates of birth, residential addresses, employee name, employee surname, email addresses, telephone numbers, gender, salary and pension details, direct manager, employment start date, termination date, marital status, number of children, personal email, emergency contact name, emergency contact phone, a record of sick days, certain medical information, work schedule, department, annual leave allowance, date and times of absences from work, reasons for absence from work

(ii) correspondence between Processor and Controller and Controller Users

(iii) navigational data (including website usage information, location and traffic data, weblogs, resources you access, IP address, online identifier and other communication data)

Controller represents and warrants that:

(a) Controller has the right to transfer such Personal Data (including Sensitive Personal Data, if applicable) to Processor for the purpose of receiving the Service; and

(b) Controller is solely responsible for obtaining all required consents, authorisations and permissions from such Users and third parties and providing all required notifications to such Users and third parties (where applicable) to enable you to provide such information to Processor.

(c) Subject-Matter and Nature of the Processing. The subject-matter of Processing of Personal Data by Processor is the provision of the Services to Controller that involves the processing of Personal Data.

(d) Purpose of the Processing. Personal Data will be processed for the purpose of providing the services set out and otherwise agreed to in the Agreement, including:

(i) administration and management of Controller account;

(ii) providing Controller with an end user support;

(iii) moderation and initial setup of the Account;

(iv) research and analytics purposes to improve the quality of the Service;

(v) ensuring the security for Controller and other users of the Service;

(vi) sending to Controller further information about Services based on a request from Controller;

(vii) providing Controller with notification of any changes to the Service.

(e) Duration of the Processing. Personal Data will be processed for the duration of the Agreement and the period from expiry of the Agreement until deletion of all Controller's Personal Data by Processor in accordance with this DPA.

Controller Responsibility

Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to Processor and the processing of Personal Data.

This DPA is Controller's complete and final instruction to Processor in relation to Personal Data and any additional instructions outside the scope of DPA would require prior written agreement between the parties.

Processor Responsibility

Compliance with Instructions. The parties acknowledge and agree that Client is Controller of Personal Data and Calamari is Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller's instructions. If Processor believes that an instruction of Controller infringes the Data Protection Laws, it shall immediately inform Controller.

Data Protection Officer. Processor appoints Data Protection Officer who performs his/her duties in compliance with Articles 38 and 39 of GDPR. Controller can contact DPO at any time via email dpo@calamari.io.

Security. Processor shall take the appropriate technical and organizational security measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, but are not be limited to described under "Technical and organizational security measures" section. Processor shall implement measures of data security to ensure a level of security appropriate to the risk concerning the confidentiality, integrity, availability and resilience of the systems within the meaning of Article 32 Paragraph 1 of GDPR.

Confidentiality. Processor shall ensure that any personnel whom Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the above-entitled activities.

Personal Data Breaches. Processor will notify Controller as soon as practicable (but no later than 72 hours) after it becomes aware of any of any Personal Data Breach affecting any Personal Data.

At Controller's request, Processor will promptly provide Controller with all reasonable assistance necessary to enable Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Laws.

Personal Data Breaches notification may include:

(a) the nature of the Data Breach;
(b) the date and time upon which the Data Breach took place and was discovered;
(c) the number of Data Subjects affected by the incident;
(d) the categories of Personal Data involved;
(e) the name and contact details of the DPO contact.

Data Subject Requests. Processor will provide reasonable assistance to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Laws with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law.

If Data Subject request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subject to submit their request to Controller. Controller shall be solely responsible for responding to any Data Subjects requests.

Sub-Processors. Controller authorises Processor to appoint sub-processors as they deem appropriate or necessary for the provision of the services in accordance with this DPA.

Before onboarding Sub-processor, Processor conducts a verification of the security and privacy practices and Data Protection Laws compliance of Sub-processor. If Processor intends to introduce a new Sub-processor other than the companies listed in "Sub-processors list", Processor will notify Controller thereof in writing (email to the email address(es) on record in Processor's account information for Controller is sufficient), including the name and location of the relevant sub-processor and the activities it will perform, and will give Controller the opportunity to object to the engagement of the new sub-Processors within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if Controller proves that significant risks for the protection of its Personal Data exist at the sub-Processor). If Processor and Controller are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party.

Data Location and Data Transfers. Controller agrees that Processor may store and process Personal Data in the Republic of Poland and any other country in which Processor or any of its Sub-processors maintains facilities outside of the EEA for the purposes of providing Controller with the Service. Such countries may not have laws offering the same level of protection for Personal Data as those inside the EEA; however where such transfers of data occur, Processor will take steps to prevent the transfer of Personal Data without adequate safeguards being put in place and will ensure that Controller Users' Personal Data collected

in the EEA and transferred internationally is afforded the same level of protection as it would be inside the EEA (according to the Article 46 of GDPR).

The location of the Controllers data storage will be automatically chosen during the registration process based on a country selected during that process. The default location of Personal Data for Controllers located in the European Economic Area ("EEA") is the data center in Ireland. The list of Processor data centers is available at help.calamari.io.

Integrations. Controller is able to turn on the integration of Services with third party applications. By turning on the integration, Controller agrees to transfer Personal Data to a third party application according to the purpose of the integration. Processor will provide Controller with any information about the nature of the integration, including the Personal Data categories that can be transferred to the third party application. Controller shall be solely responsible for the compliance of Personal Data processing by third party application with Data Protection Laws - it is not a matter of this document.

Deletion of Personal Data. Processor will provide a possibility to delete Personal Data (including copies thereof) processed pursuant to this DPA. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further processing.

Processor will provide mechanisms for Controller to:

(a) delete a record of single Data Subject at any time
(b) delete all the Personal Data at the end of the contract
(c) support requests which may include Personal Data

The deleted Personal Data cannot be recovered by Controller (for example, from the “trash”). Processor will delete such Personal Data from its systems and backups as soon as reasonably practicable and within a maximum period of 90 days of data retention.

Audits

Controller may exercise their right to audit the technical and organizational security measures taken by Processor under GDPR legislation.

For such purpose, Controller may, e.g.,

- obtain information from Processor,
- request Processor to submit to Controller an existing attestation or certificate by an independent professional expert, or
- upon reasonable and timely advance agreement, during regular business hours and without interrupting Processor’s business operations, conduct an on-site inspection of Processor’s business operations or have the same conducted by a qualified third party which shall not be a competitor of Processor. Controller pays an applicable audit fee in full to Processor, including the internal costs of Processor, and in advance of the commencement of such audit.

Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

Changes to this DPA

If at any time Processor makes a change to this DPA, Processor will update this document to reflect such change. Processor will inform Controller at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect by either:
(a) sending an email to Controller contact email; or
(b) alerting Controller via Service user interface.

Technical and organizational security measures

Processing Infrastructure. Processor hosts its Service with outsourced infrastructure providers. Additionally, Processor maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. Processor relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors. The vendors maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Physical and Environmental Security. Processor hosts its Service infrastructure with multi-tenant, outsourced infrastructure providers. Processor ensures that tenant data it processes is kept logically and/or physically separate from all other data processed by Processor. The physical and environmental security controls of infrastructure providers are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications - details available on https://aws.amazon.com/compliance/.

Network Security. Processor uses network access control mechanisms which are designed to prevent network traffic using unauthorized protocols from reaching the Service infrastructure. The technical network security measures implemented differ between infrastructure providers and include firewall rules, DDoS protection.

Authentication. Processor implemented a uniform password policy for its Services and provides SSO authentication possibility. Users who make use of the Services via the user interface must authenticate before accessing non-public customer data.

Authorization. Controller's data is stored in multi-tenant storage systems accessible via application user interfaces and application programming interfaces only. Controllers are not allowed direct access to the underlying application infrastructure. The authorization model in Processor Services is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options.

Application Programming Interface (API) access. Public product APIs may be accessed using an API key.

Privacy by Design. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks, Processor implements data-protection principles in an effective manner and to integrate the necessary safeguards.

(a) services are protected against attacks such as SQL injections, CSRF tokens, XSS, and designed according to the best practices;
(b) reviews of code stored in Processor's source code repositories is performed, checking for coding best practices and identifiable software flaws. Processor draws on industry experience both internal and external to ensure source code is readable and maintainable;

(c) Processor implemented an automated test suites to verify the quality of code.

Firewall and Antivirus. Processor implements appropriate firewall, anti-virus, anti-spyware and other anti-malware software and technologies on all networks and systems it uses to process personal data. Processor updates its firewall, anti-virus, anti-spyware and other anti-malware software and technologies on a regular basis.

Incident Detection and Monitoring. Processor follows a consistent incident management process. Processor is continuously improving the process to reduce the impact of incidents, decrease the amount of time it takes to resolve it, and most importantly avoid the chance of repeat incidents.

Backup and Redundancy. Processor's infrastructure systems have been designed to minimise the impact of anticipated environmental risks. Services are designed to perform certain types of preventative and corrective maintenance with the minimum interruption. Controller data is backed up and using a industry standard methods to multiple durable data stores and replicated across multiple availability zones. Back-ups are stored securely and are available for data restoration within a 24 hour time period.

Encryption Technologies. Processor makes HTTPS 256-bit encryption (also referred to as SSL or TLS connection) available. Processor Services support Diffie Hellman cryptographic key exchange signed with RSA. These methods help protect traffic and minimise the impact of attacks on cryptographic security. Data storage is automatically encrypted to protect your data at rest.

Businesses Continuity. Processor replicates data over multiple systems and locations to help to protect against accidental destruction or loss. Processor has designed and regularly plans and tests its business continuity and disaster recovery programs.

Personnel Security. Processor's personnel is required to conduct themselves in a manner consistent with the Processor's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Processor conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Processor's confidentiality and privacy policies.

A subset of Processor's employees have access to Controller's data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged.

In case of any questions regarding the details of implemented technical and organizational security measures, please contact dpo@calamari.io

Sub-processors list

Sub-processor	Purpose	Location	Website
Amazon Web Services, Inc.	Infrastructure provider, Email service provider	USA, Ireland, Singapore, United Kingdom	https://aws.amazon.com/
Google, Inc.	Email service provider, Product analytics	USA	https://www.google.com/analytics/ https://gsuite.google.com
Intercom, Inc.	Communication chat provider	USA	https://www.intercom.com
HubSpot, Inc.	CRM provider	USA	https://www.hubspot.com
Slack Technologies, Inc.	Support team communication	USA	https://slack.com
Tawk.to Inc.	Communication chat provider	USA	https://www.tawk.to
The Rocket Science Group, LLC	Email service provider	USA	https://mailchimp.com
PayPal (Europe) S.a.r.l et Cie, S.C.A	Payment provider	Luxembourg	https://www.paypal.com/
PayLane sp. z o.o	Payment provider	Poland	http://paylane.com

On behalf of Client:

Name (written out in full): _____
Position: _____
Signature: _____

On behalf of Calamari:

Name: Hubert Lisek
Position: Member of the Board
Signature: Hubert Lisek