DATA PROCESSING ADDENDUM
TO
SOFTWARE LICENSE AGREEMENT
BY
BUSINESSMAP OOD

Background:

(A) BMAP provides computer software (Kanbanize SaaS), developed by BMAP and visualized in the Website www.kanbanize.com (hereinafter "**Services**"). In providing these Services, BMAP may process personal data (as defined below) on behalf of the Client.

(B) Parties have concluded a Software license agreement regarding these Services (hereinafter referred to as the "**Agreement**"), which they now wish to amend in respect of their data processing obligations under Applicable Data Protection Law (as defined hereunder).

(C) The Parties have hereunder agreed the terms upon which BMAP will process such personal data.

1. Data Protection

1.1. *Definitions:* In this Addendum, the following terms shall have the following meanings:

(a) "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in Applicable Data Protection Law; and

(b) "**Applicable Data Protection Law**" shall mean: Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and national data protection laws.

1.2. *Relationship of the parties:* the Client (the controller) appoints BMAP as a processor to process the personal data described in the Annex: "**Data Processing Description** (the "**Data**"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

1.3. The Client shall have sole responsibility for the accuracy and legality of uploaded Data and, where the Client acquired such Data, the means by which the Client acquired Data. The Client warrants and undertakes that it has and will maintain the legal bases for processing, including all necessary consents, and notices required, where applicable, to enable BMAP to lawfully process the Data for the duration and purposes of the Services.

1.4. *Purpose limitation:* BMAP shall process the Data as a processor for the purposes described in the Annex "**Data Processing Description**" and strictly in accordance with the documented instructions of the Client (the "**Permitted Purpose**"), except where

otherwise required by Applicable Data Protection Law. In no event shall BMAP process the Data for its own purposes or those of any third party.

1.5. *International transfers:* BMAP shall not transfer the Data (nor permit the Data to be transferred) outside of the European Economic Area ("**EEA**") unless (i) it has first obtained the Client's prior written consent; and (ii) it takes such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Data to a recipient in a country that the European Commission has decided provides adequate protection for personal data, to a recipient that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law, or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission in accordance with the requirements of the European Court of Justice.

1.6. *Confidentiality of processing:* BMAP shall ensure that any person that it authorises to process the Data (including BMAP's staff, agents and subcontractors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Data who is not under such a duty of confidentiality. BMAP shall ensure that all Authorised Persons process the Data only as necessary for the Permitted Purpose.

1.7. *Security:* BMAP shall implement appropriate technical and organisational measures to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Incident**"). Such measures shall have regard to 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.

Such measures shall include, as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

At a minimum, such measures shall include the measures identified in the Annex "**Minimum Security Measures**" to this Addendum.

1.8. *Subprocessing:* BMAP shall not subcontract any processing of the Data to a third party subprocessor without the prior written consent of the Client. Notwithstanding this, the

Client consents to BMAP engaging third party subprocessors to process the Data provided that: (i) BMAP provides at least [30] days' prior notice of the addition or removal of any subprocessor (including details of the processing it performs or will perform) by sending a product update notification or an email to the Client email address or via the Admin Console of the BMAP Software; (ii) BMAP imposes data protection terms on any subprocessor it appoints that protect the Data to the same standard provided for by this Clause; and (iii) BMAP remains fully liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor. Client email addresses to be used for notification:

_____

1.9. A list of approved subprocessors as at the date of this Addendum is attached in the **Annex "Approved Subprocessors"**, and BMAP shall maintain and provide updated copies of this list to the Client when it adds or removes subprocessors in accordance with this Clause.

1.10. If the Client refuses to consent to BMAP's appointment of a third party subprocessor on reasonable grounds relating to the protection of the Data, then either BMAP will not appoint the subprocessor or the Client may elect to suspend or terminate this Addendum/ the Agreement or the respective Service without penalty for the Client at any time.

1.11. *Cooperation and data subjects' rights:* BMAP shall provide all reasonable and timely assistance (including by appropriate technical and organisational measures) to the Client at its own expense to enable the Client to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to BMAP, BMAP shall inform the Client within 48 hours providing full details of the same.

1.12. *Data Protection Impact Assessment:* If BMAP believes or becomes aware that its processing of the Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall promptly inform the Client and provide the Client with all such reasonable and timely assistance as the Client may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

1.13. *Security incidents:* Upon becoming aware of a Security Incident, BMAP shall notify the controller without undue delay after becoming aware of a personal data breach, and shall provide all such timely information and cooperation as the Client may require in order to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. BMAP shall further take promptly and without undue delay all such measures and actions as are necessary to remedy or

mitigate the effects of the Security Incident and shall inform the Client of all developments in connection with the Security Incident.

1.14. *Deletion or return of Data:* Upon termination or expiry of the Agreement, BMAP shall destroy or return to the Client all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for processing) within 4 weeks. This requirement shall not apply to the extent that BMAP is required by any EU (or any EU Member State) law to retain some or all of the Data, in which event BMAP shall isolate and protect the Data from any further processing except to the extent required by such law.

1.15. *Audit:* BMAP shall permit the Client (or its appointed third party auditors) to audit BMAP's compliance with this Clause, and shall make available to the Client all information, systems and staff necessary for the Client's (or its third party auditors) to conduct such audit. BMAP acknowledges that the Client (or its third party auditors) may enter its premises for the purposes of conducting this audit, provided that the Client gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to BMAP's operations. The Client will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) the Client believes a further audit is necessary due to a Security Incident suffered by BMAP. BMAP may charge a fee (based on BMAP's reasonable costs) for any audit. BMAP will provide the Client with further details of any applicable fee, and the basis of its calculation, in advance of any such review or audit.

1.16. *Indemnity:* Each Party (the "**Indemnifying Party**") shall indemnify the other (the "**Indemnified Party**") from and against all loss, cost, harm, expense (including reasonable legal fees), liabilities or damage ("**Damage**") suffered or incurred by the Indemnified Party as a result of the Indemnifying Party's breach of the data protection provisions set out in this Clause, and provided that: (i) the Indemnified Party gives the Indemnifying Party prompt notice of any circumstances of which it is aware that give rise to an indemnity claim under this Clause; and (ii) the Indemnified Party takes reasonable steps and actions to mitigate any ongoing Damage it may suffer as a consequence of the Indemnifying Party's breach. Regardless of the above, nothing in this DPA will affect the terms of the applicable Agreement relating to liability (including any specific exclusions from and any limitation of liability).

Annex "Data Processing Description"

This Annex describes the processing that BMAP will perform on behalf of the Client.

Purpose and Nature of the processing

Processing activities are performed for the purpose of and in relation to providing the Services through the BMAP software, including storage, processing and use of Data for the purpose of providing the Services, providing technical support, communication in regard to use of Services and related activities.

Data uploaded by BMAP software users, defined by the Client as data on strategies, measures, projects, campaigns, initiatives, tasks, changes, responsibility, dates and times, as well as any other data which the Users choose to enter into the software, not indicated in the Categories of data below, if any, shall be stored by BMAP within the scope of the Services.

Each party shall be entitled to store, use and process contact details, provided by the other party, with the purpose of establishing communications between the parties, in regard with the administration and fulfillment of the contract.

Data subjects

The personal data to be processed concern the following categories of data subjects:

- Users of the BMAP Software

Categories of data

The personal data to be processed concern the following categories of data:

CATEGORIES OF PERSONAL DATA PROCESSED	Yes/No
Identification Data (name, email address, job position, telephone number)	Yes
Electronic identification data (IP addresses, device identifier, cookies)	Yes
Location data (GSM, GPS)	No
Financial characteristics (account number, credit/debit card details, earnings)	No
Personal characteristics (age, gender, civil status, date of birth, place of birth)	No
Economic and financial information (income, financial situation, tax situation, etc.)	No
Physical data (height, weight, hair colour, eye colour, distinctive features)	No

Lifestyle data (consumption of alcohol/tobacco, consumption of goods and services, information about travel, social contacts, etc.)	No
Psychological data (personality, character)	No
National Ids and identifiers (e.g. social security numbers)	No
Household composition (marital status and details, spouse/partner details, number of children, household/family members)	No
Leisure activities and interest (hobbies, sports, other interests)	No
Affiliations (charities, volunteering, clubs, but excluding political or trade union affiliations)	No
Education and training (educational history, professional qualification and experience, professional organisations, publications)	No
Profession and job (employment details, employer, job title, recruitment details, career, attendance and discipline, occupational health, salary, company assets held, evaluation, training)	No
Online tracking and usage data	No
Other	No

Special categories of data

The personal data to be processed concern the following special categories of data:

SENSITIVE DATA	**Yes/No**
Data revealing ethnic or racial origin	No
Data revealing political opinions	No
Data revealing religion or philosophical beliefs	No
Data revealing trade union membership	No

Genetic data	No
Biometric Data	No
Health data / medical data	No
Data concerning sex life or sexual orientation	No
Data relating to criminal convictions or offences	No

Annex "Approved Subprocessors"

For Clients who have opted to use the EU Amazon Web Services, BMAP shall not use the services of US Amazon Web Services.

Type	Subrocessor	EU / Non-EU	Client Data	Comment
Email server	Superhosting	EU	Email-related data	
Hosting	Amazon Web Services	EU	All Tier II data	Data center in Ireland. Client can request to move the Data to the EU data center.
Hosting	Amazon Web Services	USA	All Tier II data	Data center in USA. This is the default data center.

Annex "Security Measures"

SECURITY AREAS	SECURITY MEASURES FOR PERSONAL DATA PROTECTION
NETWORK AND SYSTEMS SECURITY	Firewall and router configurations are set-up, in order to restrict the traffic, inbound and outbound, from “untrusted” networks (including wireless) and hosts. Deny all other traffic except, for protocols necessary for the personal data environment (PDE).
	Application firewalls are set-up in front of web servers belonging to PDE, in order to verify and validate the traffic which is directed to the server. Any unauthorized service or traffic should be blocked and an alert should be generated.
	Production (real) data is only allowed in production environments. Upon exception and with all necessary approvals, QA environments may process (real) personal data only to the extent that they are protected as production environments. The environment of testing and development, as well as pre-production environments must use either anonymized or synthetic data.
	Standard hardening configuration templates have to be developed for databases, applications, operating systems and applications containing personal data.
DATA SECURITY	Personal data retention time must be limited to the extent which is necessary for each single processing activity, albeit in compliance with legal and/or regulatory (retention) obligations.
	Personal data has to be made unreadable (e.g. leveraging on encryption), when stored on portable digital media, backup media, log files.
	Strong cryptography and security protocols have to be implemented, in order to protect personal data during the transmission over open, public or untrusted networks.
	In case the channel encryption is not possible, files and attachments containing personal data have to be protected by means of encryption whenever they are transmitted over open, public or untrusted networks.
	Security tools are used to monitor and control the flow of personal data through endpoints and towards external networks.
	Databases/data storages encryption are based upon a proper classification of assets in scope, according to the level of criticality. As a sample, databases/data storages serving bank’s core business

	processes/services or storing a large amount of personal data may be protected by strong encryption.
	Media containing personal data must be protected against unauthorized access, through adequate physical (e.g. lock) and logical (e.g. encryption, access control, etc.) security measures.
	Upon return and/or dismissal of ICT assets and resources, secure clean-up procedures (e.g. wiping) are put in place, in order to remove all personal data and/or securely overwrite prior to disposal or re-use.
	Paper documents or magnetic/optical media (e.g.: hard disks, DVDs, CDs, smart cards, USB flash drives) have to be destroyed or rendered unusable to ensure that the data and information they contain cannot be reconstructed and/or used (even partially) by unauthorized Third Parties. Paper documents have to be physically destroyed before being trashed, through specific shredder devices.
	Employees are adequately educated and trained on the correct rules of conduct to be adopted for the protection of personal data contained in paper documents (example: in case of removal from the workstation make sure that nobody can access confidential information, protect the original documents and the photocopies from theft or unauthorized use, keep the documentation in drawers and closets locked at the end of the working session)
DATA AVAILABILITY	Proper procedures are put in place in order to restore the availability of personal data (as a right of the data subject) in a timely manner. Back-up procedures should ensure copies of personal data at least weekly.
IDENTITY AND ACCESS MANAGEMENT	Access authorization to production environments containing personal data is given according to the "need to know" and “least privilege” principles.
	Policies and procedures are implemented to ensure the proper identification of users and administrators accessing system components managing personal data. All users are assigned with a unique user name before allowing them to access system components or personal data.
	Individual remote administrative accesses to systems managing personal data are protected, by means of an authentication mechanism requiring password changes every 90 days. Additionally, password vaulting tools should be evaluated in order to increase credentials' security.

	Passwords for systems and devices managing personal data must contain at least 8 digits, not easily attributable to the user, and they must be changed at least every 3 months.
	System resources and access right must be assigned to user accounts, where user accounts are assigned to unique users.
	Remote access (from external networks) to PDE have to be protected by means of multi-factor authentication.
	All accesses to databases containing personal data are protected/controlled as follows: - Application credentials to access databases cannot be used by individual users or other non-application processes - Such application/system user credentials must be appropriately protected against potential misuse. - Access must be granted only to the personnel who really needs it for the performance of own job/tasks (need to know principles) - A formal user registration and de-registration process are implemented to enable assignment of access rights to manage personal data.
	Number of personal data repositories (databases, files, copies, archives) is kept to an absolute minimum, avoiding unnecessary duplication. Instead of duplication, preference should be given to pseudonymised databases, that perform look-ups into master repositories for specific personal data, if, and when needed.
	Visibility of personal data must be limited to the sole set of information which is necessary for the single processing activities. No unnecessary personal data should be made available to users.
	Users' access rights to personal data is reviewed/re-certified at regular intervals and, in any case, at least annually – as per the regular Identity and Access Management process.
	Administrators are required to access a system using a fully logged and non-administrative account. Then, once logged onto the machine without administrative privileges, the administrator should gain administrative privileges.
LOGGING AND MONITORING	Access to production environments containing personal data - and where technically possible access to personal data – are monitored and logged, in order to precisely record the link between access and individual user accessing personal data
	Adequate procedures are put in place to ensure the continuous availability of personal data: back-up personnel is identified to

ORGANISATION AND HUMAN SECURITY	ensure the continuity of the service to the data subject willing to access own personal data.
	A formal security awareness program is implemented, to make all personnel aware of policy and procedures related to personal data security. Periodic tests or simulations may be performed, to assess whether employees click on a link from suspicious e-mail or provide personal/sensitive information without following appropriate security procedures to verify the reliability of the source. As a consequence, targeted training is provided to those employees falling victim to the test.
	Clear contractual agreements have to be signed-off with service providers, in order to state their responsibility for the security of personal data they process/store/transmit on behalf of the Data Controller.
	Employees responsibilities and duties on the confidentiality of personal data are clearly stated as valid also after the termination or change of employment.
	Personal data must not be copied on removable media, except from those media expressly authorized by the Processor for specific tasks.
DATA PROTECTION BY DESIGN	Processes and tools for the Secure Software Development Lifecycle (SDLC) are integrated with appropriate security check/controls and requirements, in order to ensure that new ICT software/applications are designed and developed taking into consideration the requirements of embedded security.
	Processes of ICT Change Management are integrated with appropriate security check/controls and requirements, in order to ensure the continuous protection of ICT software/applications in place, upon relevant changes.
PERSONAL DATA BREACH NOTIFICATION	Processes and tools for Incident Management are properly implemented and/or improved, in order to enable the detection and classification of personal data breaches so that they are correctly communicated to the Controller within the terms established in the paragraph “Notification obligation and Security Breach“.
	A register of personal data breaches is created and maintained.