

DATA PROCESSING AGREEMENT

Last updated 29th November 2024

This Data Processing Agreement (“DPA”, “Agreement”) is an addendum to and forms part of the master agreement between the Administrator of Bitrix24 Customer Account and Alaio (<https://www.bitrix24.com/terms/>) to reflect the parties’ agreement for the provision of the Processor Services (as amended from time to time) and processing of Bitrix24 Customer Account User’s Personal Data in accordance with the requirements of the Data Protection Legislation.

This Data Processing Agreement will be effective from the Effective Date.

BY CLICKING THE "I ACCEPT" BUTTON BELOW, YOU (A) ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT; (B) REPRESENT AND WARRANT THAT YOU HAVE THE RIGHT, POWER, AND AUTHORITY TO ENTER INTO THIS AGREEMENT; AND (C) ACCEPT THIS AGREEMENT AND AGREE THAT YOU ARE LEGALLY BOUND BY ITS TERMS.

APPLICATION OF THIS DPA

If there is any conflict or inconsistency between the terms of this DPA and the Terms of Service (<https://www.bitrix24.eu/terms/>), the DPA will govern. Subject to the amendments in this DPA, the Terms of Service remain in full force and effect.

THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

1. INTRODUCTION

This DPA reflect the parties’ agreement on the terms governing the processing and security of User Personal Data in connection with the Data Protection Legislation.

1.1 DEFINITIONS AND INTERPRETATION

“**Alaio**” shall have the meaning according to the Contracting Party section of Alaio (former Bitrix24) Terms of Service (<https://bitrix24.com/terms/>) depending on the domain zone registration of your customer account, the following legal entities will be your Data Controllers:

- a) Alaio Cloud Limited a company registered under the laws of the Republic of Cyprus with its registered office at Frema House, office 102, No. 9, Constantinou Papparigopoulou Str., 3106, Limassol, Cyprus;
- b) Alaio Inc. a company organized under the laws of the Commonwealth of Virginia, United States of America with its registered address at 700 North Fairfax St., Suite 614-B, Alexandria, VA 22314, USA; and

c) Bitrix24 India Private Limited with its registered office address is B-01, Prestige Centre Point, Edward Road, H.K.P.Road, Bangalore, Bangalore North, Karnataka, India, 560054, and its affiliates

(collectively, "Alaio", "We", "Us" "Our" or "Bitrix24").

“Administrator” means user having administrative privileges as defined in the Terms of Service (<https://www.bitrix24.eu/terms/>).

“Bitrix24” means; Bitrix24 website, products and services provided by Alaio as specified in Bitrix24 terms of service (<https://www.bitrix24.com/terms/>).

“User Personal Data” means personal data that is processed by Alaio on behalf of the Administrator as part of Alaio provision of the Processor Services.

“Data Incident” means a breach of Bitrix24 security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, User Personal Data on systems managed by or otherwise controlled by Alaio. “Data Incidents” will not include unsuccessful attempts or activities that do not compromise the security of User Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“Data Protection Legislation” means all legislation and regulatory requirements in force from time to time relating to the use of personal data and the privacy of electronic communications including, but not limited to: EU 2016/679 General Data Protection Regulation (GDPR); California Privacy Rights Act of 2020 and any other USA applicable federal and state privacy legislation; General Data Protection Law (Law No. 13.709/2018 of Brazil, (Lei Geral de Proteção de Dados); Law No. 30 of 2018 on the Protection of Personal Data of Bahrein; the federal Privacy Act 1988 of Australia; Personal Information Protection and Electronic Documents Act of Canada; The Personal Information Protection Law of China; Personal Data (Privacy) Ordinance (Cap. 486) of Hong Kong; Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 of India; Digital Personal Data Protection Act of India; Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) of Indonesia; Government Regulation No. 71 of 2019 on the Provision of Electronic Systems and Transactions (Electronic Systems Regulation) of Indonesia; Ministry of Communications and Information Technology (MCI) Regulation No. 20 of 2016 on Personal Data Protection in an Electronic System (Personal Data Regulation) of Indonesia; Protection of Privacy Law (5741-1981) of Israel; Act on the Protection of Personal Information of Japan; Personal Data Protection Act 2010 (PDPA of Malaysia; Privacy Act 1993 of New Zealand; The Data Privacy Act of 2012 (Republic Act No. 10173) of Philippines; Law No.13 of 2016 Promulgating the Protection of the Privacy of Personal Data Law of Qatar; The Personal Data Protection Act 2012 of Singapore; The Protection of Personal Information Act 2013 of South Africa; Personal Information Protection Act of South Korea; Federal Data Protection Act of 19 June 1992 (Switzerland), Personal Data Protection Act of Taiwan; Law on Protection of Personal Data No. 6698 of Turkey; Law No. 18,331 on Personal Data Protection and Habeas Data Action as amended by Laws No. 18,719 and 18,996 of Uruguay; Decree No. 414/009 regulating the PDPL of Uruguay.

“Effective Date” means, as applicable:

The date on which User clicked to accept or the parties otherwise agreed to this DPA.

“Notification Email Address” means Primary email addresses associated with your account used by the first administrator for portal registration, used also to receive certain notifications from Bitrix24 relating to these Data Processing Terms or used for email authentication.

“Personal Data” means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

“Processing of personal data” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (“Process”, “Processes” and “Processed” shall have the same meaning).

“Security measures” means measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing as described in the document (or the applicable part dependent on what Services Administrator purchases from Bitrix24), as updated from time to time, and accessible via the link in the Appendix 2 to this DPA.

“Processor Services” means the provision of maintenance and support services, consultancy or professional services and the provision of software as a service or any other services provided under the Agreement where Bitrix24 Processes Personal Data on behalf of the Administrator.

“Sub-processors” means third parties authorized by Bitrix24 to have logical access to and process Personal Data in order to provide parts of the Processor Services and any related technical support.

“Service provider” means any entity operated for profit that “processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract.

“Term” means the period from the Effective Date until the end of Bitrix24 provision of the Processor Services to Administrator under the Agreement.

“User” means any user of Bitrix24 Customer Account with or without administrative privileges as defined in Terms of Service (<https://www.bitrix24.eu/terms/>).

The terms **“Data controller”**, **“Data subject”**, **“Personal data”**, **“Processing”**, **“Data processor”** and **“Supervisory authority”** as used in this DPA have the meanings given in the Data Protection Legislation.

2. PROCESSING OF PERSONAL DATA

2.1 Roles and Regulatory Compliance; Authorization.

2.1.1 Processor and Controller Responsibilities. The parties acknowledge and agree that:

- (a) Appendix 1 to the Agreement describes the subject matter and details of the processing of Personal Data;
- (b) Alaio is a processor (service provider under the California Privacy Rights Act of 2020 and any other applicable federal and state USA privacy legislation) of Personal Data under the applicable Data Protection Legislation;
- (c) Administrator is a controller or processor, as applicable, of Personal Data under the Data Protection Legislation; and
- (d) each party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Personal Data;
- (e) Administrator shall, in its use or receipt of the Services, Process Personal Data in accordance with the requirements of Data Protection Legislation and will ensure that its instructions for the Processing of Personal Data shall comply with Data Protection Legislation. Administrator shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Administrator acquired Personal Data. Alaio will inform the Administrator immediately if it believes that a data processing instruction violates the GDPR or other data protection provisions of the Union or the Member States.

2.2 Authorization by Third Party Controller. If Administrator is a processor, Administrator warrants to Alaio that its instructions and actions with respect to Personal Data, including its appointment of Alaio as another processor, have been authorized by the relevant controller.

2.3 The parties agree that with regard to the Processing of Personal Data, Alaio or members of the Alaio Group will engage Sub-processors pursuant to the requirements set forth in Section 7 "Sub-processors" below.

2.4 By entering into this Data Processing Agreement, Administrator instructs Alaio to process Personal Data only in accordance with applicable law: (a) to provide the Processor Services and any related technical support; (b) as further specified via Administrator's use of the Processor Services (including in the settings and other functionality of the Processor Services) and any related technical support; (c) as documented in this Data Processing Agreement; and (d) as further documented in any other written instructions given by Administrator and acknowledged by Bitrix24 as constituting instructions for purposes of this Data Processing Agreement.

2.5 Deletion on Term Expiry. On expiry of the Term, Administrator instructs Alaio to delete all Personal Data (including existing copies) from Bitrix24 systems in accordance with applicable law. Alaio will comply with this instruction as soon as reasonably practicable and within a maximum period of 90 days, unless any applicable law requires storage.

2.5.1 Account deletion. Paid plans devolve to the free plan according to the process described above. If the Bitrix24 Customer Account is on a free plan (either converted to a free plan or originally on a free plan) and is completely inactive over the course of 30 days, it is 'archived', and it can be retrieved only by an administrator account (yourself or a user in the instance with administrator rights). To retrieve the account, a User without administrative rights simply needs to log in.

If no User logs in for another 15 days after the instance has been 'archived', Bitrix24 Customer Account will be deleted.

2.5.2 The Administrator may initiate deletion of the Bitrix24 Customer Account by first dismissing other Administrators, if any, which will entail deletion of all the connected User Accounts and all connected User Content, subject to the availability of such feature. In this case, Bitrix24 Customer Account will be made inactive immediately and completely deleted over the course of 90 (ninety) calendar days. However, this operation will not delete completely User's Bitrix24 network accounts which will remain active for use in another Bitrix24 Customer Accounts.

3. DURATION OF THIS DPA

This DPA will take effect on the Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all User Personal Data by Bitrix24 as described in this DPA.

4. RIGHTS OF DATA SUBJECTS

4.1 If the Administrator, in its use or receipt of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Legislation, Alaio will (taking into account the nature of the processing of Personal Data and, if applicable, Article 11 of the GDPR) assist Administrator in fulfilling any obligation of Administrator to respond to requests by data subjects, including (if applicable) Administrator's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR and other Data Protection Legislation, by providing the functionality of the Processor Services;

4.2 Alaio shall, to the extent legally permitted, promptly notify Administrator if it receives a request from a Data Subject for access to, correction, amendment, restriction, deletion or exercising any other rights under the GDPR or other Data Protection Legislation of that person's Personal Data. Alaio shall not respond to any such Data Subject request without Administrator's prior written consent except to confirm that the request relates to User. Alaio shall provide Administrator with cooperation and assistance in relation to handling of a Data Subject's request for access to that person's Personal Data or exercising any other rights under the GDPR or other Data Protection Legislation, to the extent legally permitted and to the extent User does not have access to such Personal Data through its use or receipt of the Services.

5. PERSONNEL

5.1 Alaio shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality as described in the Appendix 2 to this DPA and such obligations survive the termination of that persons' engagement with Alaio.

5.2 Alaio shall ensure that Alaio Group's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

6. DATA SECURITY

6.2 Alaio Security Measures. Alaio will implement and maintain technical, physical and organisational measures to protect confidentiality and integrity of Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in the Appendix 2 to this DPA (the “Security Measures”). As described in the Appendix 2 to this DPA, the Security Measures include measures: (a) to help ensure the ongoing confidentiality, integrity, availability and resilience of Bitrix24 systems and services; (b) to help restore timely access to personal data following an incident; and (c) for regular testing of effectiveness. Alaio may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

6.3 Security Compliance by Alaio Staff. Alaio will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of performance, including ensuring that all persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality as described in the Appendix 2 to this DPA.

6.4 Alaio Security Assistance. Administrator agrees that Alaio will assist in ensuring compliance with any obligations of Administrator in respect of security of personal data and personal data breaches, including (if applicable) Administrator’s obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

- (a) implementing and maintaining the Security Measures in accordance with the Appendix 2 to this DPA;
- (b) complying with the terms of Section 8 (Data Incidents); and
- (c) providing User with the Security Documentation.

7. SUB-PROCESSORS

7.1 Consent to Sub-processor Engagement. Administrator specifically authorizes that Alaio is engaging a number of third-party Sub-processors in connection with the provision of the Service (also accessible via Bitrix24 Infrastructure, Sub-processors and joint controllers).

7.2 Requirements for Sub-processor Engagement. When engaging any Sub-processor, Alaio will:

- (a) ensure via a written contract that:
 - (i) the Sub-processor only accesses and uses Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this DPA); and
 - (ii) if the GDPR applies to the processing of Personal Data, the data protection obligations set out in Article 28(3) of the GDPR are imposed on the Sub-processor;
- (b) Alaio have entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor; and
- (c) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Sub-processor.

7.4 Objection Right for New Sub-processors.

When any new Sub-processor is engaged during the Term, and if the GDPR applies to the processing of Personal Data, Alaio will, at least 10 days before the new Sub-processor processes any Personal Data, inform Administrator of the engagement (including the name

and location of the relevant sub-processor and the activities it will perform) by sending an email to the Notification Email Address.

Administrator may object to any new Sub-processor by notifying Alaio promptly in writing within five (5) business days after receipt of Alaio notice. In the event Administrator objects to a new Sub-processor, Alaio will use reasonable efforts to make available to Administrator a change in the Services or recommend a commercially reasonable change to Administrator's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the User. If Alaio is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Administrator may terminate the applicable Order with respect only to those Services which cannot be provided by Alaio without the use of the objected-to new Sub-processor by providing written notice to Alaio. Alaio will refund Administrator any prepaid fees covering the remainder of the term of such Order following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Administrator.

8. DATA INCIDENTS.

8.1 Incident Notification. If Alaio becomes aware of a Data Incident, Alaio will: (a) notify Administrator of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize the harm and secure Personal Data.

8.2 Details of Data Incident. Notifications will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Alaio recommends Administrator take to address the Data Incident.

8.3 Delivery of Notification. Alaio will deliver its notification of any Data Incident to the Notification Email Address or, at Bitrix24 discretion, by other direct communication (for example, by phone call or an in-person meeting). Administrator is solely responsible for ensuring that the Notification Email Address is current and valid.

8.4 Third Party Notifications. Administrator is solely responsible for complying with breach notification laws applicable to Administrator and fulfilling any third party notification obligations related to any Data Incident.

8.5 No Acknowledgement of Fault by Alaio. Alaio notification of or response to a Data Incident will not be construed as an acknowledgement by Alaio of any fault or liability with respect to the Data Incident.

9. INSPECTIONS OF COMPLIANCE

9.1 To demonstrate compliance by Alaio with its obligations under this DPA, and upon Administrator's request, Alaio will provide more detailed information on the security measures described in the Appendix 2 to this DPA.

9.2 Upon Administrator's request, and subject to the confidentiality obligations set forth in this DPA, Alaio shall make available to User that is not a competitor of Alaio (or Administrator's independent, third-party auditor that is not a competitor of Bitrix24) information regarding Alaio compliance with the obligations set forth in this DPA and the security measures as described in the Appendix 2 to this DPA. Administrator may contact Alaio to request an on-site inspection of the architecture, systems and procedures relevant to the protection of Personal Data at locations where Personal Data is stored. Administrator shall reimburse Alaio for any time expended by Alaio or its third-party Sub-processors for any such on-site inspection at the Alaio then-current professional services rates, which shall be made available to Administrator upon request. Before the commencement of any such on-site audit, Administrator and Alaio shall mutually agree upon the scope, timing, and duration of the inspection in addition to the reimbursement rate for which Administrator

shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Alaio, or its third-party Sub-processors. Administrator shall promptly notify Alaio with information regarding any non-compliance discovered during the course of an inspection.

10. DATA PROTECTION IMPACT ASSESSMENT

Upon Administrator's request, Alaio will assist Administrator in ensuring compliance with any obligations of Administrator in respect of data protection impact assessments and prior consultation, including (if applicable) Administrator's obligations pursuant to Articles 35 and 36 of the GDPR, to the extent User does not otherwise have access to the relevant information, and to the extent such information is available to Alaio. Alaio shall provide reasonable assistance to Administrator in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks.

11. DATA TRANSFERS

11.1 Data storage geography depending on Alaio (Bitrix24) domain zone is described in the Alaio [Infrastructure, Sub-processors and joint controllers section](#).

All Data obtained via Bitrix24.eu, Bitrix24.de, Bitrix.it, Bitrix24.pl, Bitrix24.uk and Bitrix24.fr domain zones is processed by Alaio Cloud Limited registered on Republic of Cyprus inside the European Union Economic Area and hosted inside the European Union in Frankfurt, Germany by Amazon Web Services data centers, which are fully GDPR compliant - <https://aws.amazon.com/blogs/security/...dpr-ready/>

11.2 For more information about data processing activities related to Users registered through the domain names Bitrix24.com, Bitrix24.com.br, Bitrix24.in, Bitrix24.tr, Bitrix24.cn, Bitrix24.cn/tc, Bitrix24.mx, Bitrix24.co, Bitrix24.vn, Bitrix24.id, Bitrix24.jp, Bitrix24.com/my, Bitrix24.com/th, Bitrix24.com.tr, please see [Alaio Infrastructure, Sub-processors and joint controllers section](#).

11.3 International transfers.

11.3.1 Alaio may process User Personal Data in Russian Federation subject to appropriate safeguards under article 46 GDPR (see schedule 11.4) and in the USA (see schedules 11.3.2 and 11.3.3)

11.3.2 Specific for data transfers from EU, UK and Switzerland to the USA, Alaio, Inc complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Alaio, Inc has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Alaio, Inc has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this DPA and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>. The Data Privacy Framework (DPF) list of participating organisations is available at

<https://www.dataprivacyframework.gov/s/participant-search>. Under certain conditions, you can invoke the corresponding binding arbitration.

The Federal Trade Commission has jurisdiction over Alaio, Inc compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

11.3.3 Disputes resolution

Alaio, Inc Internal Complaints Mechanism In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Alaio, Inc commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU, UK and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF should first contact Alaio, Inc at: privacy@bitrix24.com

Alternative Dispute Resolution Body

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Alaio, Inc commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF to JAMS, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit <https://www.jamsadr.com/> for more information or to file a complaint. The services of JAMS are provided at no cost to you.

11.4 The security of data and the data subject rights under GDPR for the data processing activities in Russian Federation are protected by appropriate safeguards under article 46 GDPR, specifically by the Standard Contractual Clauses adopted by the European Commission in accordance with the examination procedure. European Commission decided that standard contractual clauses offer sufficient safeguards on data protection for the data to be transferred internationally. You have a right to request information on those contractual safeguards (Please contact our Data Protection Officer).

12. GOVERNING LAW

12.1 This DPA (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of Republic of Cyprus.

12.2 Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of Republic of Cyprus.

12.3 For data transfers outside the EEA listed in schedules 11.3.4 protected by appropriate safeguards under article 46 GDPR, specifically by the standard data protection clauses adopted by the Commission in accordance with the examination procedure from controllers in the EU to processors established outside the EU and Users when the processing is in the context of the activities of an establishment of EEA countries other than Republic of Cyprus and/or Users offering services to data subjects who are in the EEA countries other than Republic of Cyprus the lead supervisory authority is Republic of Cyprus under article 56

GDPR.

The supervisory authority of the single establishment of Alaio within the EEA competent to act as lead supervisory authority for the cross-border processing carried out by that processor in accordance with the procedure provided in Article 60 of GDPR is the supervisory authority of Cyprus.

13. CHANGES TO THIS DPA

13.1 Alaio may change this DPA if the change:

- (a) is expressly permitted by this DPA;
- (b) reflects a change in the name or form of a legal entity;
- (c) is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency; or
- (d) does not: (i) result in a degradation of the overall security of the Processor Services; (ii) expand the scope of, or remove any restrictions on, Bitrix24 processing of Personal Data; and (iii) otherwise have a material adverse impact on User's rights under this DPA, as reasonably determined by Bitrix24.

13.2 Notification of Changes. If Alaio makes any updates to this DPA, Alaio will inform Administrator by either: (a) sending an email to the Notification Email Address; or (b) alerting Administrator via the user interface for the Processor Services. If Administrator objects to any such change, Administrator may terminate the Agreement by giving written notice to Alaio within 30 days of being informed by Alaio of the change.

Appendix 1

SUBJECT MATTER AND DETAILS OF THE DATA PROCESSING SUBJECT MATTER

Data Subjects. The personal data transferred concern the following categories of data subjects.

1. Data subjects about whom Alaio collects personal data in its provision of the Processor Services; and/or
2. Data subjects about whom personal data is transferred to Alaio in connection with the Processor Services by, at the direction of, or on behalf of Administrator.

Including:

- Staff including volunteers, agents, temporary and casual workers
- Users and clients (including their staff)
- Suppliers (including their staff)
- Members or supporters
- Complainants, correspondents and enquirers

- Advisers, consultants and other professional experts

Categories of data The personal data transferred concern the following categories of data:

- Personal details, including any information that identifies the data subject and their personal characteristics, including: first and last name, business contact details;
- Communications metadata
- Employment data which may include: working time, geolocation (under user's consent as part of working time tracking)
- Goods or services provided and related information, including details of the goods or services supplied, licences issued, and contracts
- Location country, city, state and region
- Online identifiers
- Device identifiers
- Documents structured data
- Personal images, audio and video recordings
- Lifestyle and social circumstances
- Signatures

Special categories of data (if appropriate):

N/A

Processing operations The personal data will be subject to the following basic processing activities (please specify):

- IT, digital, technology or telecom services, including provision of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software licensing. Including, but not limited to:
- Collecting, recording, organizing, structuring, storing, retrieving, using, disclosing, erasing and destroying) User Personal Data for the purpose of providing the Services and any related technical support to User in accordance with this Data Processing Agreement. The services include the following: Social Intranet, Project Management and Tasks, Chat and Video, Document Management and Bitrix24.Drive, Calendars, Mail, CRM, Sites, Open Channels, Contact center,

Telephony, Time management, CRM marketing, Workflows, eCommerce, Box version.

Appendix 2

SECURITY MEASURES

Alaio will implement and maintain the Security Measures set out in this Appendix 2. Alaio may update or modify such Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

1. KEY PRINCIPLES OF THE DATA PROTECTION BY BITRIX24

- 1.1 All Alaio IT Systems are protected against unauthorised access.
- 1.2 All Alaio IT Systems are used only in compliance with relevant Company Policies.
- 1.3 All Alaio employees and any third parties authorised to use the IT Systems including, but not limited to sub-processors, must ensure that they are familiar with this Policies and must adhere to and comply with it at all times.
- 1.4 All line managers ensure that all employees and sub-processors under their control and direction adhere to and comply with this Policies at all times as required under paragraph 2.3.
- 1.5 All data stored on IT Systems are managed securely in compliance with all relevant parts of EU Regulation 2016/679 General Data Protection Regulation (“GDPR”) and all other laws governing data protection whether now or in the future in force.
- 1.6 All data stored on IT Systems is classified appropriately. All data so classified is handled appropriately in accordance with its classification.
- 1.7 All data stored on IT Systems is available only to those Users with a legitimate need for access.
- 1.8 All data stored on IT Systems is protected against unauthorised access and processing.
- 1.9 All data stored on IT Systems is protected against loss and corruption.
- 1.10 All breaches of security pertaining to the IT Systems or any data stored thereon are reported and subsequently investigated by the IT Department.

2. SOFTWARE SECURITY MEASURES

- 2.1 All software in use on the IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) are kept up-to-date and any and all relevant software updates, patches, fixes, and other intermediate releases are applied.

- 2.2 Where any security flaw is identified in any software that flaw is fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied.
- 2.3 No Alaio employees may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the IT Manager. Any software must be approved by the IT Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

3. ANTI-VIRUS SECURITY MEASURES

- 3.1 Alaio IT Systems (including all computers and servers) are protected with suitable anti-virus, firewall, and other suitable internet security software. All such software is kept up-to-date with the latest software updates and definitions.
- 3.2 All Alaio IT Systems protected by anti-virus software are subject to a full system scan at least once a week.
- 3.3 All physical media (e.g. USB memory sticks or disks of any kind) used by employees for transferring files must be virus-scanned before any files may be transferred. Such virus scans are performed by the IT Staff Manager.
- 3.4 Alaio employees are permitted to transfer files using cloud storage systems only with the approval of the IT Manager. All files downloaded from any cloud storage system are scanned for viruses during the download process.
- 3.5 Any files being sent to third parties outside the Company, whether by email, on physical media, or by other means (e.g. shared cloud storage) are scanned for viruses before being sent or as part of the sending process.

4. HARDWARE SECURITY MEASURES

- 4.1 Alaio IT Systems are located in rooms which are securely locked (with authorised Users being granted access by means of a smart card).
- 4.2 All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment, and network infrastructure) are located in secured, climate-controlled rooms in locked cabinets which may be accessed only by designated members of the IT Department.
- 4.3 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company are always transported securely and handled with care.

5. ACCESS SECURITY

- 5.1 Access privileges for all IT Systems is determined on the basis of employee levels of authority within Alaio Company organization structure and the requirements of their job roles. Employees are not granted access to any IT Systems or electronic data which are not reasonably required for the fulfilment of their job roles.
- 5.2 All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) are protected with a secure password or passcode, or such other

form of secure log-in system as the IT Department may deem appropriate and approve.

5.3 All passwords are covered with the following security measures:

- a) Are at least 8 characters long;
- b) Contain a combination of upper and lower case letters, numbers, symbols;
- c) Changed at least every 90 days;
- d) Different from the previous password;
- e) Not obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.); and
- f) Created by individual Users.

5.4 All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) are protected with a password protected screensaver that will activate after 5 minutes of inactivity.

6. DATA STORAGE SECURITY

- 1.1 All data, and in particular personal data is stored securely using passwords and OTP authorization.
- 1.2 No personal data is stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Bitrix24 or otherwise.
- 1.3 No data, and in particular personal data, is transferred to any computer or device personally belonging to an employee unless the employee in question is a sub-processor working on behalf of Alaio and that employee has agreed to comply fully with the Company's Data Protection Policy and the GDPR.

7. DATA PROTECTION

7.1 All personal data (as defined in the GDPR) collected, held, and processed by Alaio is collected, held, and processed strictly in accordance with the principles of the GDPR, the provisions of the GDPR and the Company's Data Protection Policy.

7.2 All Users handling data for and on behalf of Alaio are subject to, and must comply with, the provisions of the Company's Data Protection Policy at all times. In particular, the following shall apply:

- a) All emails containing confidential or sensitive personal data are encrypted using TLS SSL protocol;
- b) All emails containing confidential or sensitive personal data are marked "confidential";
- c) Confidential and sensitive personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;

- d) All confidential and sensitive personal data to be transferred physically, including that on removable electronic media, is transferred in a suitable container marked “confidential”.
- e) Where any confidential or sensitive personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the employee must lock the computer and screen before leaving it.

7.3 Any questions relating to data protection should be referred to the Data Protection Officer Elena Riazanova (info@quick-gdpr.co.uk).

8. DATA CENTERS & NETWORK SECURITY OF THE HOSTING PROVIDER

Alaio uses Amazon Web Services to store and analyze data, including AWS Cloud infrastructure in Europe (Frankfurt) Region and Europe (Ireland) Region.

AVAILABILITY

AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS Users can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

BUSINESS CONTINUITY PLAN

The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

MEDIA DESTRUCTION

Media storage devices used to store User data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored User data is not removed from AWS control until it has been securely decommissioned.

INFRASTRUCTURE MAINTENANCE

Equipment maintenance. AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

Environment management. AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

GOVERNANCE & RISK

Data Center risk management. The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

Third-party security attestation. Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

(b) Networks & Transmission.

Data Transmission. Alaio Datacenters are connected via private links protected by AWS Network firewalls to provide secure data transfer. This is designed to protect the confidentiality, integrity and availability of the network and prevent data from being read, copied, altered or removed without authorization during electronic transfer.

Data Breach Response. Alaio monitors a variety of communication channels for security breaches, and Alaio security personnel will react promptly to known incidents.

External Attack Surface. Alaio considers potential attack vectors and incorporates appropriate purpose built proprietary technologies into external facing systems.

Encryption Technologies. Alaio uses HTTPS encryption (also referred to as SSL or TLS connection).

9. SUBPROCESSOR SECURITY

Before onboarding Sub-processors, Alaio conducts an audit of the security and privacy practices of Sub-processors to ensure Sub-processors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Alaio has assessed the risks presented by the Sub-processor then, subject always to the requirements set out in Section 7 the Sub-processor is required to enter into appropriate security, confidentiality and privacy contract terms.

