





tamigo

Data Processing
Agreement

Controller

Code:	GDPR Tamigo 7.5
Version:	9 
Date of Version:	September 17 th , 2018 FysioDanmark Vejle Sjællandsgade 23A · 7100 Vejle
Created by:	Henrik K. Nielsen Tlf. 75 83 22 12 · CVR-nr. 29814538
Approved by:	
Confidentiality level:	Public
Geographical scope:	The European Union (EU) & EEA

This Data Protection Agreement ("Agreement"), forms part of the Service Agreement ("Principal Agreement") between:

Customer Name 
FysioDanmark Vejle
Sjællandsgade 23A · 7100 Vejle
(hereinafter referred as the "Controller") acting on its own behalf **Tlf. 75 83 22 12 · CVR-nr. 29814538**

And

tamigo ApS
Kristianiagade 8
2100 København Ø
(hereinafter referred as the "Processor") acting on its own behalf.

If a Principal Agreement exists, the terms and conditions set out below shall be added as a Supplementary Agreement to the Principal Agreement. In this case terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. If no Principal Agreement exist, this Agreement shall have effect as the Agreement between the parties.

01 Definitions

In this Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

"Authorised Sub-processors" means (a) those Sub-processors set out in Annex 2 (Authorised Transfers of Controller Personal Data); and (b) any additional Sub-processors consented to in writing by Controller in accordance with Sub-processing section.

"Sub-processor" means any Data Processor (including any third party) appointed by the Processor to process Controller Personal Data on behalf of the Controller.

"Process/Processing/Processed", "Data Controller", "Data Processor", "Data Subject", "Personal Data", "Special Categories of Personal Data" and any further definition not included under this Agreement or the Principal Agreement shall have the same meaning as in EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR").

"Data Protection Laws" means EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR").

"Erasure" means the removal or destruction of Personal Data.

"EEA" means the European Economic Area.

"Third Country" means any country outside EU/EEA, except where that country is the subject of a valid adequacy decision by the European Commission on the protection of Personal Data in Third Countries.

"Controller Personal Data" means the data described in Annex 1 and any other Personal Data processed by Processor on behalf of the Controller pursuant to or in connection with the Principal Agreement.

"Personal Data Breach" means a breach of leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Controller Personal Data transmitted, stored or otherwise processed.

"Services" means the services to be supplied by the Processor to the Controller pursuant to the Principal Agreement.

"Products" means the products to be supplied by the Processor to the Controller pursuant to the Principal Agreement.

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to Processors established in third countries, as approved by the European Commission Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these.

02 Data Processing Terms

2.1 In the course of providing the Services and/or Products to the Controller pursuant to the Principal Agreement, the Processor may process Controller Personal Data on behalf of the Controller as per the terms of this Agreement. The Processor agrees to comply with the following provisions with respect to any Controller Personal Data.

2.2 To the extent required by applicable Data Protection Laws, the Processor shall obtain and maintain all necessary licenses, authorizations and permits necessary to process personal data including personal data mentioned in Annex 1.

The Processor shall maintain all the technical and organizational measures to comply with the requirements set forth in the Agreement and its Annexes.

03 Processing of Controller Personal Data

- 3.1 The Processor shall only process Controller Personal Data for the purposes of the Principal Agreement. The Processor shall not process, transfer, modify, amend or alter the Controller Personal Data or disclose or permit the disclosure of the Controller personal data to any third party other than in accordance with Controller's documented instructions, unless processing is required by EU or Member State law to which Processor is subject. The Processor shall, to the extent permitted by such law, inform the Controller of that legal requirement before processing the Personal Data and comply with the Controller's instructions to minimize, as much as possible, the scope of the disclosure.
- 3.2 For the purposes set out in section above, the Controller hereby instructs the Processor to transfer Controller Personal Data to the recipients in the Third Countries listed in Annex 2 (Authorised Transfers of Controller Personal Data), always provided that Processor shall comply with section sub-processors.

04 Reliability and Non-Disclosure

- 4.1 The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Controller Personal Data, ensuring in each case that access is strictly limited to those individuals who require access to the relevant Controller Personal Data.
- 4.2 The Processor must ensure that all individuals which have a duty to process Controller Personal Data:
 - 4.2.1 Are informed of the confidential nature of the Controller Personal Data and are aware of Processor's obligations under this Agreement and the Principal Agreement in relation to the Controller Personal Data;
 - 4.2.2 Have undertaken appropriate training in relation to the Data Protection Laws or any other training;
 - 4.2.3 Are subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and
 - 4.2.4 Are subject to user authentication and logon processes when accessing the Controller Personal Data in accordance with this Agreement, the Principal Agreement and the applicable Data Protection Laws.

05 Personal Data Security

- 5.1 Taking into account 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, the Processor shall implement appropriate technical and organizational measures (Annex 3) to ensure a level of Controller Personal Data security appropriate to the risk, including but not limited to:
 - 5.1.1 Pseudonymization and encryption;
 - 5.1.2 The ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;
 - 5.1.3 The ability to restore the availability and access to Controller Personal Data in a timely manner in the event of a physical or technical incident; and
 - 5.1.4 A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.
- 5.2 In assessing the appropriate level of security, the Processor shall take into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Controller Personal Data transmitted, stored or otherwise processed.

06 Sub-Processing

- 6.1. As of the Agreement Effective Date, the Controller hereby authorises the Processor to engage those Sub-Processors set out in Annex 2. The Processor shall not engage any Data-Sub-Processors to Process Controller Personal Data other than with the prior written consent of Controller, which Controller may refuse with absolute discretion.
- 6.2. With respect to each Sub-processor, the Processor shall:
 - 6.2.1. Provide the Controller with full details of the Processing to be undertaken by each Sub-processor.
 - 6.2.2. Carry out adequate due diligence on each Sub-Processor to ensure that it can provide the level of protection for Controller Personal Data, including without limitation, sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of GDPR, this Agreement, the Principal Agreement and the applicable Data Protection Laws.
 - 6.2.3. Insofar as that contract involves the transfer of Controller Personal Data outside of the EEA, incorporate the Standard Contractual Clauses or such other mechanism as directed by the Controller into the contract between the Processor and each Sub-Processor to ensure the adequate protection of the transferred Controller Personal Data.
 - 6.2.4. Remain fully liable to the Controller for any failure by each Sub-Processor to fulfil its obligations in relation to the Processing of any Controller Personal Data.

07 Data Subject Rights

- 7.1. Taking into account the nature of the Processing, the Processor shall, at an hourly fee according to the current standard price list, assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising Data Subject rights as laid down in EU GDPR.
- 7.2. The Processor will direct a Data Subject to the Controller if it receives a request from a Data Subject, the Supervisory Authority and/or other competent authority under Data Protection Laws with respect to Controller Personal Data.
- 7.3. The Processor shall cooperate as requested by the Controller to enable the Controller to comply with any exercise of rights by a Data Subject under any Data Protection Laws with respect to Controller Personal Data and comply with any assessment, enquiry, notice or investigation under Data Protection Laws with respect to Controller Personal Data or this Agreement, which shall include:
 - 7.3.1. The provision of all data requested by the Controller within any reasonable timescale specified by the Controller in each case, including full details and copies of the complaint, communication or request and any Controller Personal Data it holds in relation to a Data Subject.
 - 7.3.2. Where applicable, providing such assistance as is reasonably requested by the Controller to enable the Controller to comply with the relevant request within the timescales prescribed by the Data Protection Laws.
 - 7.3.3. Implementing any additional technical and organisational measures as may be reasonably required by the Controller to allow the Controller to respond effectively to relevant complaints, communications or requests.

08 Personal Data Breach

- 8.1. The Processor shall notify the Controller without undue delay and, in any case, no later than 24 (twenty-four) hours after becoming aware of or reasonably suspecting a Personal Data Breach. The Processor will provide the Controller with sufficient information to allow the Controller to meet any obligations to report a Personal Data Breach under the Data Protection Laws. Such notification shall as a minimum:
 - 8.1.1. Describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
 - 8.1.2. Communicate the name and contact details of the Processor's Data Protection Officer, Privacy Officer or other relevant contact from whom more information may be obtained;
 - 8.1.3. Describe the estimated risk and the likely consequences of the Personal Data Breach; and
 - 8.1.4. Describe the measures taken or proposed to address the Personal Data Breach.
- 8.2. The Processor shall co-operate with the Controller and take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each Personal Data Breach.
- 8.3. In the event of a Personal Data Breach, the Processor shall not inform any third party without first obtaining the Controller's prior written consent, unless notification is required by EU or Member State law to which the Processor is subject, in which case the Processor shall, to the extent permitted by such law, inform the Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Controller before notifying the Personal Data Breach.

09 Data Protection Impact Assessment and Prior Consultation

The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments which are required under Article 35 of GDPR and with any prior consultations to any supervisory authority of the Controller which are required under Article 36 of GDPR, in each case solely in relation to Processing of Controller Personal Data by the Processor on behalf of the Controller and considering the nature of the processing and information available to the Processor.

10 Erasure or return of Controller Personal Data

- 10.1. This DPA shall automatically terminate upon any termination or expiration of the Agreement or upon Data Controller's request. The Parties agree that at termination or expiry of the Agreement, Data Processor shall, at the choice of Data Controller, delete and/or return all data processed under the Agreement and the DPA, including copies. Upon Data Controller's request, Data Processor shall also provide documentation for such deletion.
- 10.2. Processor may retain Controller Personal Data to the extent required by Union or Member State law, and only to the extent and for such period as required by Union or Member State law, and always provided that Processor shall ensure the confidentiality of all such Controller Personal Data and shall ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) specified in the Union or Member State law requiring its storage and for no other purpose.

11 Audit rights

For an hourly fee according to the current standard price list, the Processor shall make available to the Controller, upon request, all information necessary to demonstrate compliance with this Agreement and allow for, and contribute to audits, including inspections by the Controller or another auditor mandated by the Controller of any premises where the Processing of Controller Personal Data takes place. For an hourly fee according to the current standard price list the Processor shall permit the Controller, or another auditor mandated by the Controller to inspect, audit and copy any relevant records, processes and systems in order that the Controller may satisfy itself that the provisions of this Agreement are being complied with. The Processor shall provide full cooperation to the Controller with respect to any such audit and shall, at the request of the Controller, provide the Controller with evidence of compliance with its obligations under this Agreement. Processor shall immediately inform the Controller if, in its opinion, an instruction pursuant to this section infringes the GDPR or other EU or Member State data protection provisions.

Processor shall nevertheless bear the costs if an audit reveals non-compliance with the processing agreement or the General Data Protection Regulation (GDPR).


12 International Transfers of Controller Personal Data

- 12.1. Processor shall not process Controller Personal Data nor permit any Authorised Sub-processor to process the Controller Personal Data in a Third Country, other than with respect to those recipients in Third Countries (if any) listed in Annex 2 (Authorised Transfers of Controller Personal Data), unless authorized in writing by Controller in advance, via an amendment to this Agreement.
- 12.2. When requested by Controller, Processor shall promptly enter into (or procure that any relevant Sub-processor of Processor enters into) an agreement with Controller including Standard Contractual Clauses and/or such variation as Data Protection Laws might require, in respect of any processing of Controller Personal Data in a Third Country, which terms shall take precedence over those in this Agreement.

13 General Terms

- 13.1. Subject to this section, the parties agree that this Agreement and the Standard Contractual Clauses shall terminate automatically upon termination of the Principal Agreement or expiry or termination of all service contracts entered into by the Processor with the Controller, pursuant to the Principal Agreement, whichever is later.
- 13.2. Any obligation imposed on the Processor under this Agreement in relation to the Processing of Personal Data shall survive any termination or expiration of this Agreement.
- 13.3. This Agreement, excluding the Standard Contractual Clauses, shall be governed by the governing law of the Principal Agreement for so long as that governing law is the law of a Member State of the European Union.
- 13.4. With regard to the subject matter of this Agreement, in the event of inconsistencies between the provisions of this Agreement and any other agreements between the parties, including but not limited to the Principal Agreement, the provisions of this Agreement shall prevail with regard to the parties' data protection obligations for Personal Data of a Data Subject from a Member State of the European Union.
- 13.5. Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding part of the Principal Agreement with effect from the Agreement Effective Date first set out above.



Signature

Agreed for and on behalf of Processor

Henrik K. Nielsen

Print Name

Data Protection Officer

Title

Tuesday, 18 September 18

Date



Signature

Agreed for and on behalf of Controller

KRISTOFFER DALSGAARD

Print Name

DIREKTØR

Title

Date

2/10 2019.



FysioDanmark Vejle
Sjællandsgade 23A · 7100 Vejle
Tlf. 75 83 22 12 · CVR-nr. 29814538

ANNEX 1: DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Controller Personal Data

The subject matter and duration of the Processing of the Controller Personal Data are set out in the Principal Agreement and this Agreement.

The purpose of the Processing of Controller Personal Data

Workforce Management & employee administration

The types of Controller Personal Data to be Processed (only Controller applicable data will be processed):

- Contact details
- Work history
- National data
- Contract details
- Bank details
- Time and attendance
- Absences
- Location
- Identity papers
- Confidential personal information
- Marital status
- Gender
- Union membership
- Disability

The categories of Data Subject to whom the Controller Personal Data relates

Employees

Personal data is subject to the following processing activities:

- Creation
- Updating
- Transmission (only if export to e.g. a Pay-Roll system)
- Calculation
- Storage
- Deletion

ANNEX 2: AUTHORISED TRANSFERS OF CONTROLLER PERSONAL DATA

List of Approved Sub-processors as at the Agreement Effective Date to be included here.

Please include (i) full legal name; (ii) processing activity; (iii) location of service centre(s).

No.	Authorized sub-processor	Processing activity	Location of service centre
1.	Azure	Employee Administration, Data Center	Netherlands
2.	Mail Chimp	Employee Communication	US (under EU-U.S. Privacy Shield Framework)
3.	SendInBlue	Employee Communication	EU
4.	ZenDesk	support	EU
5.	MS Office 365	Administration	EU
6.	Link Mobility	Employee Communication	EU/EEA
7.	Typeform	Customer Surveys	EU & US (under EU-U.S. Privacy Shield Framework)

ANNEX 3: ORGANISATIONAL & TECHNICAL MEASURES

As a company tamigo takes your data security and privacy very seriously, we recognize that our information security practices are important to you. While we don't like to expose too much detail around our practices we have provided some general information below to give you confidence in how we secure the data entrusted to us.

Data Center Security

1. tamigo delivers planning of millions of hours a month for 100.000's of users. We use multiple databases, placed in a world-class data center in the Netherlands .
2. Our data center manage physical security 24/7/365 with two-factor authentication biometric scanners and high resolution video surveillance systems.
3. The data center perimeter is encompassed by tall fences of steel and concrete and can only provide entrance via well-defined access points
4. The data center entrance is staffed with professional security officers

Protection from Data Loss

1. All databases are kept separate and dedicated to preventing corruption and overlap. We have multiple layers of logic that segregate user accounts from each other.
2. Account data is mirrored and regularly backed up off site.

Application Level Security

1. tamigo account passwords are hashed. If you lose your password, it can't be retrieved—it must be reset.
2. All login pages (from our website and mobile apps) pass data via TLS.
3. The entire tamigo application is encrypted with TLS.
4. Logins via the tamigo API have Token-based authentication.
5. We perform regular external security penetration tests. The tests involve high-level server penetration tests, in-depth testing for vulnerabilities inside the application, and social engineering drills.
6. We make 2-Factor Authentication available to our customers.
7. We provide the ability to establish tiered-levels (roles) of access within accounts.
8. Certain changes to your account, such as to your password, will trigger email notifications to the account owner.

Internal IT Security

1. tamigo offices are secured by access control.
2. Our office network is heavily segmented and centrally monitored.
3. We have a dedicated internal security team that constantly monitors our environment for vulnerabilities. They perform penetration testing and social engineering exercises on our environment and our employees. Our security team includes ISO 27001 provisional implementer certified members.

Business Principles

1. We continuously train employees on data security practices, including how to identify social engineering, phishing scams, and hackers.
2. All employees (not only those who have access to customer data such as tech support and our developers) undergo criminal record checks prior to employment.