BIOSENCY
Caring anytime, anywhere

DATA PROTECTION ANNEX

1. INTRODUCTION

The Data Protection Annex (hereinafter “DPA” or “Agreement”) aims to govern the use of the personal data of the Client, who acts as data controller (hereinafter the “Client”), by Biosency, who acts as data processor (hereinafter the “Subprocessor”) under the contract (hereinafter the “Contract”).

The DPA is an integral part of the Contract signed between the Client and the Subcontractor. Under this Contract, the Subcontractor provides the Client with a Solution that involves the processing of personal data on behalf of the Client. In the event of a contradiction between the Contract and the DPA, the obligations provided for in the DPA shall prevail with regard to the applicable data protection rules.

All data protection terms used in the DPA (e.g. controller, processor, etc.) are defined in Article 4 of the General Data Protection Regulation (“GDPR”).

2. STATEMENT

The Subcontractor declares that it complies with all applicable data protection rules, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("GDPR") and Law No. 78-17 of 6 January 1978 on information technology, files and freedoms, together referred to as "applicable data protection rules".

The Subcontractor declares that it provides all sufficient guarantees to meet the requirements of the applicable data protection rules and, more particularly, to guarantee the confidentiality and protection of the Client's data.

The Subcontractor declares that all of its employees required to process the Client's personal data are bound by a confidentiality clause or by any other legal act (e.g.: rules of good conduct, information systems charter, etc.) allowing the confidentiality of the Client's personal data to be guaranteed.

The Subcontractor declares that it regularly trains and raises awareness among its employees on the applicable rules regarding data protection.

3. INSTRUCTIONS

The Subcontractor undertakes to use the Client's personal data only on the latter's documented instructions.

The Client undertakes to inform the Subcontractor of any changes to the instructions which may be made regarding the use of its personal data.

The Subcontractor must notify the Client, as soon as possible, if the latter's documented instructions constitute a violation of the applicable data protection rules.

4. COMPLIANCE BY DEFAULT AND BY DESIGN

The Subcontractor provides its service as is, in compliance with i) conformity of the service from the design stage and (ii) the conformity of the default service.

The Subcontractor provides a service accompanied by all the functionalities enabling the Client to comply with its obligations as data controller.

Consequently, the Subcontractor is never responsible for the non-compliant use of the service by the Client with the applicable data protection rules.

5. SECURITY

The Subcontractor undertakes to guarantee the security of the Client's personal data and to implement all technical and organizational measures necessary to prevent any risk of data breach.

6. DATA BREACH

The Subcontractor undertakes to notify the Client, as soon as possible and within 48 working hours after becoming aware of it, of any data breach which may concern the Client's personal data.

The Subcontractor undertakes to provide the Client, in accordance with the provisions of Article 28 of the GDPR, with all information necessary for the processing of the data breach by the Client.In the event of a data breach, the Subcontractor undertakes to take all necessary measures to remedy and reduce the impact of the breach on the Client’s personal data.

Unless expressly agreed in advance and in writing by the Client, the Subcontractor is not authorized to take charge of data breach notifications to the French supervisory authority, the CNIL. Similarly, the Subcontractor is not, in principle, authorized to inform on behalf of the Client the persons concerned by the processing carried out within the framework of the Contract.

7. SECURITY HELP AND ASSISTANCE

The Subcontractor shall provide the Client, upon written request, with all necessary and required information on the technical and organizational security measures to be implemented to guarantee the security of its personal data.

The Subcontractor shall communicate to the Client, upon written request, all necessary and required information to ensure the performance of an impact analysis (“AIPD”) directly linked to the service provided.

The Subcontractor is not, however, required to ensure or audit the Client's security or to carry out impact analyses ("AIPD") in place of and on behalf of the Client. Any additional request to the communication of information may be subject to refusal and, possibly, to an additional fee-based service.

8. HELP AND ASSISTANCE IN MATTERS OF THE RIGHTS OF PERSONS CONCERNED

The Subcontractor shall provide the Client, upon written request, with all necessary and required information to enable the Client to fulfil its obligation to respond to requests from the persons concerned.

The Subcontractor shall, upon written request from the Client, carry out the technical actions to be undertaken so that the Client can fulfil its obligation to respond to requests from the persons concerned.

The Subcontractor is not, however, required to manage requests for personal rights in place of and on behalf of the Client. Any additional request to ensure such management may be subject to refusal and, possibly, to an additional fee-based service.

9. SUBSEQUENT SUBCONTRACTORS

In general, the Client accepts that the Subcontractor recruits subsequent Subcontractors within the framework of the execution of the Contract provided that it informs the Client of any changes concerning the addition or replacement of these subsequent Subcontractors occurring during the execution of the Contract.

The Customer may raise objections by registered letter with acknowledgement of receipt i) if the Subsequent Subprocessor is one of its competitors, ii) if the customer and the Subsequent Subprocessor are in a pre-litigation or litigation situation, and iii) if the Subsequent Subprocessor has been the subject of a conviction by a data protection supervisory authority within the year of its recruitment by the Subprocessor. Each of these situations must be demonstrated.

In the event that the objection is admissible, the Subcontractor has a period of 6 months from receipt of the objection to modify the subsequent Subcontractor or to ensure compliance with the applicable data protection rules by this subsequent Subcontractor.

In all cases, the Subcontractor undertakes to recruit only subsequent Subcontractors who provide the necessary and sufficient guarantees to ensure the security and confidentiality of the Client's personal data.

In this respect, the Subcontractor undertakes i) to regularly monitor its subsequent Subcontractors and ii) to ensure that the contract concluded with the subsequent Subcontractor used in the context of the service contains obligations similar to those provided for in the DPA.

In any event, the Subcontractor remains liable for the actions of the subsequent Subcontractor under the Contract.

10. FATE OF PERSONAL DATA

The Client informs the Subcontractor, in writing and before the end of the commercial relationship, of its choice (option 1) to return the personal data to it and then delete them as well as all existing copies or, (option 2) to directly delete the personal data and all existing copies, or (option 3) to transfer the personal data to a new service provider and then delete it and all existing copies. Unless otherwise provided in the Contract, option 3 must be the subject of a quote from the Subcontractor.

In the absence of information from the Client of its choice, the Subcontractor will directly delete the Client's data as well as all copies (option 2) at the end of the commercial relationship.

The deletion of data is irreversible. The Customer is therefore invited to recover his data before the service is stopped. In the event of deletion of the Customer's data by the Subcontractor, the Customer remains solely responsible for the disappearance of the data and any consequences that may occur.

The Subcontractor certifies to the Client, upon written request, the effective deletion of personal data and all existing copies.

11. AUDITS

The Client has the right to carry out an audit in the form of a written questionnaire once a year to verify compliance with this Agreement. The questionnaire has the force of a commitment on honor which binds the Subcontractor.

The questionnaire may be communicated in any form to the Subcontractor, who undertakes to respond to it within a maximum period of two months from its receipt.

The Client also has the right to carry out an on-site audit, at its own expense, once a year only in the event of a data breach or failure to comply with applicable data protection rules and this DPA, in particular as established by the written questionnaire.

An on-site audit may be conducted either by the Client or by an independent third party designated by the Client and must be notified in writing to the Subcontractor at least thirty (30) days before the audit is carried out.

The Subcontractor has the right to refuse the choice of the independent third party if the latter is i) a competitor or ii) in pre-litigation or litigation with it. In this case, the Client undertakes to choose a new independent third party to carry out the audit.

The Subcontractor may refuse access to certain areas for reasons of confidentiality or security. In this case, the Subcontractor will carry out the audit in these areas at its own expense and communicate the results to the Client.

In the event of a discrepancy noted during the audit, the Subcontractor undertakes to implement, without delay, the measures necessary to comply with this Agreement.

12. DATA TRANSFERS OUTSIDE THE EUROPEAN UNION

The Subcontractor undertakes to do its utmost not to transfer the Client's personal data outside the European Union or to recruit a subsequent Subcontractor located outside the European Union.

However, in the event that such transfers prove necessary within the framework of the Contract, the Subcontractor undertakes to implement all the mechanisms required to supervise these transfers such as, in particular, concluding standard data protection clauses ("SCCs") adopted by the European Commission.

13. COOPERATION WITH THE SUPERVISORY AUTHORITY

When this concerns the processing implemented within the framework of the Contract, the Subcontractor undertakes to provide, upon request, all the information necessary to the Client so that it can cooperate with the competent supervisory authority.

14. CONTACT

The Client and the Subcontractor each designate a contact person who is responsible for this APD and who is the recipient of the various notifications and communications to be made within the framework of the APD.

The Subcontractor informs the Client that its Data Protection Officer can be contacted at the following contact details:

- E-mail address :dpo@biosency.com
- Postal address: Data Protection Officer, Biosency, 8 bis Rue du Pressoir Godier– 35760 Saint-Grégoire

15. REVISION

The Subcontractor reserves the right to modify this Agreement in the event of changes in the applicable data protection rules which would have the effect of modifying one of its provisions.

16. APPLICABLE LAW

Notwithstanding any provision to the contrary contained in the Contract, this Agreement is subject to French law. Any dispute relating to the performance of this Agreement shall be subject to the exclusive jurisdiction of the courts within the jurisdiction of the Court of Appeal of the place of domicile of the Subcontractor.

However, in the event that such transfers prove necessary within the framework of the Contract, the Subcontractor undertakes to implement all the mechanisms required to supervise these transfers such as, in particular, concluding standard data protection clauses ("SCCs") adopted by the European Commission.

Appendix 1 - Description of treatments

Treatments	Foundations	Persons concerned
Technical session cookies	Execution of the contract	Platform Users
Account Management	Execution of the contract	Platform Users
Accommodation	Execution of the contract	Platform users, third parties (patients)
Safety and maintenance	Legal obligation	Platform users, third parties (patients)

Appendix 2 - Description of data processed and retention periods

Data categories	Purposes	Retention periods
Connection data (see logs, IP address, etc.)	Use of the service	12 months
Identification data (name, first name)	Use of the service	Duration of the contractual relationship + 5 years (prescription)
Contact details (e.g. professional email address)	Use of the service	Duration of the contractual relationship + 5 years (prescription)
Data relating to professional life (e.g. company, position)	Use of the service	Duration of the contractual relationship + 5 years (prescription)
Banking and financial data	Use of the service	Duration of the transaction, 10 years for supporting accounting documents
Third party health data (patients)	Use of the service	Duration of the contractual relationship

Annex 3 - Technical and organizational security measures

Categories of measures	Built-in safety measures
Organizational security measure	Binding information systems charter
Organizational security measure	Employment contract clause
Organizational security measure	Awareness raising for teams twice a year
Technical security measures	Isolation of the authentication database from business data
Technical security measures	Encryption of passwords and database data at rest and during data transmission on the platform
Technical security measures	Multi-factor authentication
Technical security measures	Partitioning health data from other data
Technical security measures	Complex password required at login

Technical security measures	Secure Https platform
Technical security measures	HDS Platform

Annex 4 - List of subcontractors and transfers outside the EU

Subcontractors	Features	Server Locations	Transfers outside the EU	Appropriate guarantees	Contact details
Mailjet	Technical notifications by email	St. Ghislain, Belgium & Frankfurt, Germany	SCC via DPA	Mailjet DPA	privacy@mailgun.com.
AWS	Hosting user data Hosting of Health Data	France (Germany for backup) France (Germany for backup)	N / A	AWS DPA	Contact form: https://aws.amazon.com/fr/contact-us/compliance-support/
Twilio	Technical messages by SMS	UNITED STATES	Adequacy: Data privacy framework (DPF) BCR SCC via DPA	DPA of Twilio	privacy@twilio.com
Auth0	Authentication	Frankfurt (Dublin for backup)	SCC via DPA	DPA of Auth0	privacy@okta.com
CLARANET	Outsourcing	France	N / A	CONTRACT	dpo@fr.clara.net
iCanopy	Access to the National Health Identity service	EU	N / A	CONTRACT	https://www.icanopee.fr/solutions/produit-efficience/assistance-efficience/
YEARS	**ProSantéConnect** Authentication health professionals **Health directory** Health Professionals Directory	EU EU	N / A N / A	CONTRACT CONTRACT	https://industriels.esante.gouv.fr/contactez-nous/formulaire monserviceclient.annuaire@esante.gouv.fr
Airview by Resmed	Integration of data from VNI machines	Frankfurt, Germany Paris, France	N / A	DPA	privacy@resmed.eu