Data Processing Addendum for the ShareCRF Service

Version: 1.0
Effective date: September 28th, 2021

This Data Processing Addendum ("DPA") complements the Terms and Conditions of the ShareCRF Service between "Inetsys S.L." (hereinafter "ShareCRF") and the Client, regarding the ShareCRF Service.

1. Introduction.

This Data Processing Addendum for the ShareCRF Service, including its annexes (the "Data Processing Addendum"), will enter into force and will replace any data processing and security terms previously applicable as of the effective date of the Data Processing Addendum.

2. Definitions.

2.1 Words that begin with a capital letter have the meaning set forth below, or failing that, the meaning indicated in section 2 (Definitions) of the ShareCRF Service Terms and Conditions:

“Additional security controls" means security features, characteristics, functionality and/or controls that Client may use as desired and/or as determined, including encryption, registration, identity and access management, and access and editing permission control.

"Client Personal Data" refers to the personal data contained in the Client Data.

“EEA" refers to the European Economic Area.

"GDPR" means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

"UK GDPR" refers to the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force.

"Addendum effective date" means the date on which the Client accepted, or the parties otherwise agreed to, this Data Processing Addendum.

"Alternative transfer solution" refers to a solution, other than the Model Contractual Clauses, that allows for the legal transfer of personal data to a third country in accordance with European Data Protection Law.

“European Data Protection Law" refers to, as appropriate: (a) the GDPR; and/or (b) the Federal Data Protection Law of June 19, 1992 (Switzerland).

"Non-European Data Protection Act" refers to privacy or data protection laws in force outside the EEA, Switzerland and the United Kingdom.

"European or national law" refers to, as appropriate: (a) the legislation of the EU or EU Member States (if the EU GDPR applies to the processing of Client Personal Data); and/or (b) the law of the United Kingdom or a part of the United Kingdom (if the UK GDPR applies to the processing of Client Personal Data).

“Data Incident" refers to a violation of the security of the Service that leads to the destruction, loss, alteration, unauthorized disclosure or unauthorized access to Client Data in systems managed or controlled by ShareCRF.

“Subprocessor” means a third party authorized as another processor under this Data Processing Addendum to have logical access to and process Client Data in order to provide the Service and its support.

2.2 The terms "personal data", "data subject", "processing", "controller" and "processor", as used in this Data Processing Addendum, have the meanings given in the GDPR, regardless of whether the European Data Protection Law or the Non-European Data Protection Law are applicable.

3. <u>Duration.</u>

This Data Processing Addendum, despite the expiration of the Term, will remain in effect until ShareCRF deletes all Client Data, and will expire automatically, as described in this Data Processing Addendum.

4. **<u>Scope of the Data Protection Law</u>**

4.1 **Application of European legislation.**
The parties acknowledge that the European Data Protection Law will apply to the processing of the Client's Personal Data as indicated in the GDPR.

4.2 **Application of non-European legislation.**
The parties acknowledge that non-European data protection law may also apply to the processing of Client Personal Data.

4.3 **Application of the Data Processing Addendum.**
Except to the extent that this Data Processing Addendum states otherwise, the terms of this Data Processing Addendum will apply regardless of whether the European Data Protection Law or the Non-European Data Protection Law applies to the processing of the Client’s Personal Data.

5. **<u>Data Processing.</u>**

5.1 **Functions and regulatory compliance; Authorization.**

5.1.1 **Responsibilities of the processor and the controller.**

If the European Data Protection Law applies to the processing of the Client's Personal Data:

A. the subject and details of processing are described in Appendix 1;

B. ShareCRF is a processor of the Client Personal Data according to the European Data Protection Law;
C. Client is a controller or processor, as applicable, of that Client Personal Data according to the European Data Protection Law; and
D. Each party will comply with the obligations applicable to it under the European Data Protection Law with respect to the processing of that Client Personal Data.

5.1.2 **Authorization by the Third Party Controller.**

If the European Data Protection Law applies to the processing of Client Personal Data and the Client is a processor, the Client guarantees that its instructions and actions with respect to such Client Personal Data, including the appointment of ShareCRF as another processor, have been authorized by the relevant controller.

5.1.3 **Responsibilities under non-European law.**

If Non-European Data Protection Act applies to the processing of the Client's Personal Data by either party, the corresponding party will comply with the obligations applicable to it under that law with respect to the processing of such Client's Personal Data.

5.2 **Scope of processing.**

5.2.1 **Client's instructions.**

Client instructs ShareCRF to process Client Personal Data only in accordance with applicable law: (a) to provide the Service, support and related technical support; (b) as further specified through the use of the Service by the Client and the End Users; (c) as documented in the form of the applicable Agreement, including this Data Processing Addendum; and (d) as more fully documented in any other written instructions provided by Client and recognized by ShareCRF as instructions for the purposes of this Data Processing Addendum.

5.2.2 **ShareCRF's Compliance with Instructions.**

As of the effective date of this Data Processing Addendum, ShareCRF will comply with the instructions described in Section 5.2.1 (Client's Instructions) (including with respect to data transfers) unless European or national Legislation to which ShareCRF is subject requires other processing of Client Personal Data by ShareCRF, in which case ShareCRF will notify the Client (unless the law prohibits ShareCRF from doing so for important reasons of public interest) before the aforementioned other processing occurs.

6. **<u>Data elimination.</u>**

6.1 **Elimination during the period.**

ShareCRF will allow Client and End Users to delete Client Data during the Term in a manner consistent with the functionality of the Service.

6.2 **Elimination at the expiration of the Validity Period.**

Upon expiration or termination of the Agreement, unless expressly provided otherwise in the Agreement, the instructions are as follows:

a. If the Client requests the deletion of the data in a credible way through notification or communication, ShareCRF will delete all Client Data

from ShareCRF systems (all backup copies are excluded until such copies are deleted in the normal course of rotation backup copies) in accordance with applicable law. ShareCRF will comply with this instruction as soon as reasonably possible and within a maximum period of 180 days unless European or national legislation requires its storage.

b. If the Client does not request the deletion of the data, as indicated in the previous point, ShareCRF may retain and/or archive the Client's Data in accordance with the Good Clinical Practices Guide and taking into account the confidentiality obligations of the Agreement. ShareCRF may delete Client Data thirty (30) days after informing the customer by email. The Client may agree upon a fee with ShareCRF for the filing and retention of the “Client Data”.

Notwithstanding Section 9.1 (Access; Rectification; Restricted Processing; Portability), the Client is responsible for exporting any Client Data it wishes to retain prior to Validity Period expiration. If the Client requests assistance in exporting their Data, ShareCRF may offer this service to the Client for a reasonable fee.

6.3 **Validity of the Data Processing Addendum.**

Even if the Validity Period of the Agreement has expired and ShareCRF has eliminated the Client Data, this Data Processing Addendum will continue to apply to the Client Data so long as there is a copy of the Client Data in ShareCRF systems.

7. **<u>Data security</u>**

7.1 **ShareCRF’s security measures, controls and assistance.**

7.1.1 **ShareCRF’s security measures.**

ShareCRF will implement and maintain technical and organizational measures to protect Client Data against destruction, loss, alteration, unauthorized disclosure or accidental or illegal access, as described in Appendix 2 (the "Security Measures"). Security Measures include measures to encrypt personal data; to help ensure the confidentiality, integrity, availability, and continued resilience of ShareCRF's systems and services; to help restore timely access to personal data after an incident; and for periodic efficacy tests. ShareCRF reserves the right to update Security Measures periodically, provided that such updates do not result in degradation of the overall security of the Service.

7.1.2 **Security compliance by ShareCRF staff.**

ShareCRF: (a) will take the appropriate measures to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent that is applicable to their scope of performance, and (b) will ensure that all persons authorized to process the Client's Personal Data are under an obligation of confidentiality.

7.1.3 **Additional security controls.**

ShareCRF will make additional security controls available to: (a) allow the Client to take measures to protect the Client's Data; and (b) provide Client with information on how to protect, access and use Client Data.

7.1.4 **ShareCRF Security Assistance.**

ShareCRF (taking into account the nature of the processing of the Client's Personal Data and the information available to ShareCRF) will help the Client to guarantee compliance with its obligations in accordance with articles 32 to 34 of the GDPR by:

a. implement and maintain Security Measures in accordance with Section 7.1.1 (ShareCRF Security Measures);
b. make additional security controls available to the Client in accordance with Section 7.1.3 (Additional security controls);
c. comply with the terms of Section 7.2 (Data Incidents);
d. if subsections (a) - (c) above are insufficient for the Client to comply with such obligations, at the request of the Client, providing reasonable additional assistance. ShareCRF may charge a reasonable fee for such assistance.

7.2 **Data incidents.**

7.2.1 **Incident notification.**

ShareCRF will notify Client immediately and without undue delay after becoming aware of a Data Incident and will take reasonable steps to minimize damage and protect Client Data.

7.2.2 **Details of the Data Incident.**

ShareCRF's notification of a Data Incident will describe, to the extent possible, the nature of the Data Incident, the steps taken to mitigate potential risks, and the steps ShareCRF recommends that the Client take to address the Data Incident.

7.2.3 **Delivery of notification.**

Notifications of any Data Incident will be sent to the notification email address or, at ShareCRF's discretion, by direct communication (for example, by phone call or in-person meeting).

7.2.4 **No evaluation of Client Data by ShareCRF.**

ShareCRF has no obligation to evaluate Client Data to identify information subject to specific legal requirements. The Client is solely responsible for obeying the notification laws, incidents applicable to the Client and complying with any third party notification obligations related to any Data Incident.

7.2.5 **Non-recognition of fault by ShareCRF.**

ShareCRF's notification or response to a Data Incident under this Section 7.2 (Data Incidents) shall not be construed as an acknowledgement by ShareCRF of any fault or liability with respect to the Service.

7.3. **Client Responsibilities and Security Assessment.**

7.3.1 **Client Security Responsibilities.**

Notwithstanding ShareCRF's obligations under Sections 7.1 (ShareCRF's Security Measures, Controls and Assistance) and 7.2 (Data Incidents), and elsewhere in the applicable Agreement, Client is responsible for their use of the Service and the storage of any copies of Client Data outside of ShareCRF systems or ShareCRF Subprocessors, including:

A. use the Service and Additional security controls to ensure a risk-appropriate level of security with respect to Client Data;

B. secure the authentication credentials of the account, systems and devices used by the Client or its End Users to access the Service; and
C. retain copies of your Client Data as appropriate.

7.3.2 **Client security assessment.**

Client agrees, based on the current and intended use of the Service, that the Service, Security Measures, Additional Security Controls, and ShareCRF's commitments under this section 7 (Data Security): (a) meet the Client's needs, including with respect to any Client security obligations under European Data Protection Law and/or Non-European Data Protection Law, as applicable, and (b) provide a level of risk-appropriate security with respect to Client Data.

8. **Impact evaluations and consultations.**

ShareCRF (taking into account the nature of the processing and the information available to ShareCRF) will help the Client to guarantee compliance with its obligations in accordance with articles 35 and 36 of the GDPR, by:

a. the provision of additional security controls in accordance with Section 7.1.3 (Additional security controls) and;
b. the provision of the information contained in the applicable Agreement that includes this Data Processing Addendum; and
c. if subsections (a) and (b) above are insufficient for the Client to comply with such obligations, at the request of the Client, providing reasonable additional assistance. ShareCRF may charge a reasonable fee for such assistance.

9. **Rights of the data subject; Data export.**

9.1 **Access; Rectification; Restricted processing; Portability.**

During the Validity Period of the Agreement, ShareCRF will allow the Client, in a manner consistent with the functionality of the Service, to access, rectify and limit the processing of Client Data, including through the deletion function provided by ShareCRF as described in Section 6.1 (Deletion during the period) and to export client data.

9.2 **Data subject requests.**

9.2.1 **Client's responsibility for requests.**

During the Validity Period of the Agreement, if ShareCRF receives any request from a data subject in relation to the Client's Personal Data, and the request identifies the Client, ShareCRF will inform the data subject of the need to send their request to the Client. The Client will be responsible for responding to said request, including, where necessary, by using the functionality of the Service.

9.2.2 **ShareCRF's data subject request assistance.**

ShareCRF (taking into account the nature of the processing of the Client's Personal Data) will help the Client to comply with its obligations under Chapter III of the GDPR to respond to requests for the exercise of the rights of data subject by:

a. providing additional security controls in accordance with Section 7.1.3 (Additional security controls);
b. complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Client Responsibility for Requests); and
c. if subsections (a) and (b) above are insufficient for the Client to comply with such obligations, at the request of the Client, providing reasonable additional assistance. ShareCRF may charge a reasonable fee for such assistance.

10. **Data transfers.**

The client agrees that ShareCRF may carry out a transfer of personal data to a third country or an international organization if the European Commission has decided that the third country, a territory or one or more specific sectors of that third country, or the international organization in question, ensure an adequate level of protection. This transfer does not require specific authorization.

11. **Subprocessors.**

11.1 **Consent for the participation of the Subprocessor.**

The Client specifically authorizes the contracting as Subprocessors to those entities appearing in the effective date of this Data Processing Addendum specified in Appendix 3: List of Subprocessors. Furthermore, without prejudice to Section 11.3 (Opportunity to object to Subprocessor changes), the Client generally authorizes the hiring of any other third party as a Subprocessor (**"New Third Party Subprocessors"** hereinafter).

11.2 **Requirements for Subprocessor Engagement.**

When hiring any subprocessor, ShareCRF:

A. guarantees through a written contract that:
   i. the Subprocessor only accesses and uses the Client Data to the extent necessary to fulfill the outsourced obligations, and does so in accordance with the Agreement (including this Data Processing Addendum); and
   ii. if the GDPR applies to the processing of the client's Personal Data, the data protection obligations described in Article 28 (3) of the GDPR, as described in this Data Processing Addendum, are imposed on the Subprocessor; and
B. will remain fully responsible for all outsourced obligations and all acts and omissions of the Subprocessor.

11.3 **Opportunity to object to Subprocessor changes.**

A. When any New Third Party Subprocessors is hired during the Validity Period of the Agreement, ShareCRF, at least 30 days before the New Third Party Subprocessors begins to process customer data, will notify the Client of the engagement (including name and location corresponding subprocessor and activities).
B. The Client may, within 90 days after the notification of the hiring of a New Third Party Subprocessors, object by terminating the applicable Agreement immediately by notifying ShareCRF. This right of

withdrawal is the sole and exclusive recourse of the Client if the Client objects to any New Third Party Subprocessors.

Appendix 1: Subject and details of data processing.

Subject

Provision of the Service, in addition, to support and technical support related to the Service by ShareCRF to the Client.

Processing duration

The Validity Period plus the period from the expiration of said Validity Period until the elimination of all Client Data by ShareCRF in accordance with the Data Processing Addendum.

Nature and purpose of the processing

ShareCRF will process the Client's Personal Data for the purpose of providing the Service, in addition, to support and technical support related to Client Service in accordance with the Data Processing Addendum.

Data categories

Data relating to individuals provided to ShareCRF through the Service, by (or at the direction of) the Client or End Users.

Data subjects

Data subjects include the person's about whom data is provided to ShareCRF through the Service by (or at the direction of) the Client or End Users.

Appendix 2: Security measures

As of the effective date of the Data Processing Addendum, ShareCRF will implement and maintain the Security Measures described in this Appendix 2. ShareCRF may update or modify such Security Measures periodically provided that such updates and modifications do not result in the degradation of the overall security of the Service.

1. **IT infrastructure.**
   ShareCRF uses the services of AWS (Amazon Web Services) as computing infrastructure for processing and data storage for the Service.

   The data centers used by the ShareCRF service are located in Germany and Ireland.

The provider of this service (AWS), who acts as Subprocessor, guarantees compliance with the provisions of the GDPR. You can consult this information and the security and protection measures through this link:

https://aws.amazon.com/en/blogs/security/aws-gdpr-data-processing-addendum/

2. **Service Security.**
   ShareCRF maintains the following security measures in the Service:
   A. ShareCRF will make a full backup of Studies in the Service at least one (1) time per day.
   B. Data is encrypted at rest and in transit.
   C. Users have individual login accounts and strong passwords are required.
   D. User sessions automatically expire after the specified times if no user activity is detected:
      i. After 120 minutes for use of the eCRF web application
      ii. At 15 minutes for users accessing through ePRO access.
   E. The Client is in charge of managing the users who have access to the Study and the access level of each user.
   F. Direct access to information is restricted to key ShareCRF IT personnel, and all accesses to the different servers and services are kept in a registry.

3. **Personnel security.**
   ShareCRF personnel must conduct themselves in a manner consistent with company guidelines regarding confidentiality, business ethics, proper use, and professional standards. All personnel are required to sign a confidentiality agreement and are provided security training.

4. **Subprocessor safety.**
   Prior to onboarding the Subprocessors, ShareCRF conducts an audit of the Subprocessors' security and privacy practices to ensure that the Subprocessors provide an appropriate level of security and privacy for their access to data and the scope of services they are under. hired to toast. Once ShareCRF has assessed the risks presented by the Subprocessor, and subject to the requirements described in Section 11.2 (Requirements for Subprocessor Engagement) of this Data Processing Addendum, the Subprocessor is required to meet the appropriate security conditions, confidentiality and privacy.

Appendix 3: List of Sub-processors.

Entity Name	Purpose	Applicable Service	Country where the processing is

			carried out.
Amazon Web Services, Inc	Hosting and Infrastructure	Used as an on-demand cloud computing platform and APIs	Germany and Ireland.