

DATA PROCESSING AGREEMENT

This Agreement is part of the Contract between SINARI (hereinafter « the Processor ») and the Customer (hereinafter “the Customer”) for the purchase of the solution and associated services from SINARI (hereinafter, the “Service”). The Processor and the Customer are hereinafter collectively referred to as “the Parties”.

The Customer enters into this Agreement on its own name and, to the extent required by Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent that SINARI processes Personal Data in respect of which such Authorized Affiliates qualify as Controllers or Processors.

All words beginning with a capital letter and not specifically defined in the Contract shall be deemed to have the same meaning as in the Data Protection Laws and Regulations.

As part of the provision of the Service to the Customer in accordance with the contract, SINARI may process Personal Data on behalf of the Customer as Processor and the Parties agree to comply with the following provisions with respect to all Personal Data.

Definitions

« *Supervisory Authority* » means an independent public authority that is established by a Member State pursuant to Article 51 of the GDPR.

"*Personal data*" means any information relating to an identified or identifiable natural person.

"*Customer Data*" means all data provided by the Customer in connection with the Service.

"*Data Protection Laws and Regulations*" means Regulation 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data and “Loi Informatique et Libertés” of January 6, 1978 relating to computing, files and freedoms as amended by the Law of 20 June 2018.

"*Controller*" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

« *GDPR* » means the 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, and repealing Directive 95/46/EC (hereinafter referred to as the General Data Protection Regulation).

«*Service*» means the service provided by the Processor.

"*Processor*" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

«*Processing*» means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Object of the Contract

SINARI provides the Service to the Customer under the Contract. As part of the Service, the Parties provide that SINARI may process Customer data which may contain personal data.

The Parties agree that with regard to the Processing of personal data, SINARI acts as a Processor on behalf of the Customer, who acts either as a Data Controller or as a Processor, in which case SINARI acts as a Subprocessor.

In this context, the purpose of this Agreement is to regulate the methods of execution and organization of the Processing of this Data by the Processor.

It is understood between both Parties that the Processor acts exclusively on behalf and in accordance with the instructions of the Controller throughout the duration of this Agreement.

The Controller instructs the Processor to process the Personal Data described below in its name and on its behalf.

1 Description of the Processing(s) of Personal Data

The details of the processing operations, and in particular the categories of Personal Data and the purposes for which the Personal Data is processed on behalf of the Controller, are specified in Appendix 1 - Description of the processing of personal data. It should be noted that SINARI has created an Appendix 1 for each solution sold by the entity, allowing the Customer to consult the corresponding appendix of the solution he has subscribed to within the online documentary database of SINARI, accessible by following the link below :

<https://www.sinari.com/basedocumentaire/rgpd/dpa/annexe1>

2 Responsibilities of the Customer

The Customer shall, in the course of its use of the Service, process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirements to inform Data Subjects of the use of the Processor and obtaining the necessary consents to allow the processing of Personal Data by the Processor for the duration and purposes of the Agreement.

The Controller undertakes to :

- provide the Processor with the Personal Data referred to in point 1 of this Agreement ;
- document in writing any instructions concerning the Processing of Personal Data by the Processor;
- ensure, before and throughout the Processing, that the Processor complies with the obligations set out in the Data Protection Laws and Regulations ;
- supervise the Processing, including conduction audits and inspections of the Processor ;

The Controller is solely responsible (i) for determining the purposes and means of the Processing of Personal Data carried out by the Processor ; (ii) for the accuracy, adequacy and completeness of the aforementioned instructions. In an express and general manner, the Processor never determines the purposes and means of the processing entrusted to it by the Controller.

3 Obligations of the Parties

3.1 Instructions

The Processor shall only process Personal Data on the documented instruction of the Controller, unless it is required to do so by Union or Member State law to which it is subject. In this case, the Processor shall inform the Controller of this legal obligation prior to processing, unless prohibited

by Law on important grounds of public interest. Instructions may also be given subsequently by the Controller throughout the duration of the Processing of Personal Data.

The Processor shall immediately inform the Controller if, in its opinion, an instruction given by the Controller constitutes a breach of the Data Protection Laws and Regulations. Under no circumstances should this information be interpreted as legal advice from the Processor. The Processor reserves the right to carry out Data Processing in accordance with an instruction from the Controller that would violate the Data Protection Laws and Regulations, without this failure being considered a violation of its obligations under this Agreement.

3.2 Limitation of purpose

The Processor processes the Personal Data only for the specific purpose or purposes of the Processing, as defined in Appendix 1, unless further instructions are given by the Controller.

3.3 Duration of the Processing of Personal Data

The processing by the Processor takes place only during the period specified in Appendix 1.

3.4 Confidentiality and security of the Processing of Personal Data

Pursuant to article 32 of the GDPR, the Parties undertake to implement appropriate organizational and technical measures to ensure a level of security appropriate to the Processing. When assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing, as well as the risks to Data Subjects.

The Processor implements at least the technical and organisational measures specified in Appendix 3 to ensure the security of the Personal Data. Appendix 3 is accessible within the online documentary database of SINARI by following the link below :

<http://www.sinari.com/documentarydatabase/gdpr/dpa/TOM>

The Processor shall ensure that persons authorized to process Personal Data undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality and receive the necessary training in the protection of Personal Data.

With regard to its tools, products, applications or services, the Processor takes into account the principles of data protection by design and data protection by default.

The Processor undertakes to record the Information System (IS) maintenance operations in an event log that can be consulted by the Customer at any time. Where appropriate, each maintenance operation performed by the Processor must be the subject of a description specifying the dates, nature of the operations and the names of the people intervening.

In case of remote maintenance enabling remote access to Customer's files, the Processor shall take all steps to enable the Customer to identify the source of each external intervention. To this end, the Processor undertakes to obtain the Customer's prior agreement before any remote maintenance operation that it initiates.

The Customer remains fully responsible for the organizational and technical security measures put in place and in particular for the confidentiality of its passwords. In accordance with the Processor's standards, passwords must comply with the following recommendations:

- Impose a minimum length for passwords (medium to strong: between 12 and 14 characters, strong to very strong: at least 15);
- Do not impose a maximum length for passwords;

- Implement rules on password complexity (use of upper case, lower case, numbers and special characters);
- Choose a password without any personal or company information;
- Use a different password for each department;
- Do not save password in clear text (in a file or email, for example);
- Change default passwords;
- Impose an expiry date on passwords;
- Immediately revoke passwords in the event of suspected or proven compromise;
- Implement a password security policy;
- Implement a robustness check on passwords when they are created or renewed;
- Provide a password safe;

The Customer undertakes to transmit password to third parties, in particular Subprocessors, in a secure manner and not to transmit these passwords in clear text.

3.5 Sensitive Data

If the Processing involves Personal Data revealing racial or ethnic origin, political opinions, religious beliefs or trade-union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sex life or sexual orientation of a natural person, or data relating to criminal convictions and offences (“sensitive data”), the Processor shall apply specific limitations and/or additional guarantees.

3.6 Use of Subprocessors

The Processor shall have the general authorization of the Controller to recruit Subprocessors on the basis of an agreed list in Appendix 2 to this Agreement. The Processor shall specifically inform the Controller in writing of any proposed change to the list by the addition or replacement of Subprocessors by providing communication of the update to Appendix 2 by e-mail at least fifteen (15) days prior to the change, thereby giving the Controller sufficient time to object to the change prior to the recruitment of the Subprocessor concerned. In order to receive e-mail notifications concerning new Subprocessors, the Controller must register here:

https://www.sinari.com/newsletter_sous_traitants_ulterieus

The Processor shall provide the Controller with the information necessary to enable him to exercise his right to object. If there is no response from the Controller by the end of the aforementioned period, the Subprocessor is deemed to have been accepted.

The list of Subprocessors to the date of signature of this Agreement is set out in Appendix 2 and shall be updated by the Processor during the performance of the services, as appropriate. It should be noted that Appendix 2 lists the Subprocessors involved in the supply of each solution sold. This Appendix 2 is accessible within the online documentary database of SINARI by following the link below :

<https://www.sinari.com/documentarydatabase/gdpr/dpa/appendix2>

Where the Processor engages a Subprocessor to carry out specific processing activities (on behalf of the Controller), it will do so by means of a contract which imposes on the Subprocessor, in substance, the same data protection obligations as those imposed on the Processor under these clauses. The Processor shall ensure that the Subprocessor complies with the obligations to which it is itself subject under these clauses and the Data Protection Laws and Regulations.

The Processor shall remain fully responsible to the Controller for the performance of the obligations of the Subprocessor in accordance with the contract entered into with the Subprocessor.

3.7 Transfers of Personal Data

The Controller agrees that where the Processor recruits a Subprocessor in accordance with clause 3.6 to carry out specific Processing activities (on behalf of the Controller) and such Processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, the Processor and the Subprocessor may ensure compliance with Chapter V of the GDPR by using, in particular, the standard contractual clauses adopted by the European Commission on the basis of Article 46(2) of the GDPR, provided that the conditions for the use of such standard contractual clauses are met.

4 Assistance of the Controller by the Processor

The Processor shall assist the Controller in fulfilling its obligation to respond to the requests of data subjects to exercise their rights, taking into account the nature of the Processing.

The Processor shall inform the Controller as soon as possible of any request it has received from a data subject. It will not itself act on this request, unless authorized to do so by the Controller.

In addition to the obligation of the Processor to assist the Controller in accordance with the preceding provisions, the Processor shall also assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the Processing and the information available to the Processor.

- (1) the obligation to carry out an assessment of the impact of proposed processing operations on the protection of personal data (« data protection impact assessment ») when a type of processing is likely to present a high risk to the rights and freedoms of natural persons ;
- (2) the obligation to consult the competent supervisory authority(ies) prior to processing where a data protection impact assessment indicates that the processing would present a high risk if the Controller did not take steps to mitigate the risk ;
- (3) the obligation to ensure that Personal Data is accurate and up-to-date, by informing the Controller, without delay if the Processor becomes aware that the Personal Data it processes is inaccurate or has become obsolete ;
- (4) the obligations set out in Articles 32 to 36 of the GDPR.

5 Notification of Personal Data Breaches

The Processor undertakes to inform the Controller of any Personal Data Breach within the framework of the Service as soon as possible after becoming aware of this Personal Data Breach.

In the event of a Personal Data Breach, the Processor shall cooperate with and assist the Controller in complying with its obligations under Articles 33 and 34 of the GDPR taking into account the nature of the Processing and the information available to the Processor.

6 Documentation and compliance

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in these clauses and arising directly from the Data Protection Laws and Regulations.

At the request of the Controller, the Processor shall also allow and contribute to audits of the processing activities covered by these clauses, at reasonable intervals or in the presence of indications of non-compliance.

The Controller may decide to carry out the audit itself or to appoint an independent auditor. Audits may also include inspections of the Processor's premises or physical facilities and shall, where appropriate, be carried out with reasonable notice.

The Parties shall make the information set out in this clause, including the results of any audit, available to the competent supervisory authority(ies) upon request.

7 Return/Destruction of Processed Data

At the option of the Controller, the Processor shall delete all Personal Data or return them to the Controller at the end of the provision of services relating to the Processing, and destroy existing copies, unless Union Law or the law of the Member State requires the retention of Personal Data.

8 Processing of the Customer's Personal Data by the Processor as a Data Controller

As part of the Contract, the Processor may process Personal Data belonging to the Customer in its capacity as Data Controller.

The Data collected by the Processor is that provided by the Customer as part of the performance of the Contract and the commercial relationship maintained between the Customer and the Processor.

The Personal Data collected in this context is necessary for the performance of the Contract.

The Customer's Personal Data may be communicated to the following recipients:

- **To internal recipients** : i.e. to members of the Processor's staff who are authorized to access the Data and who strictly need it to carry out their duties ;
- **To service providers and/or Subprocessors** : hosting companies, IT service providers, etc.
- **To judicial, public or governmental authorities** : when this is necessary, for example, (i) for the Subprocessor to comply with its legal obligations, (ii) to comply with legitimate requests from public or governmental authorities, (iii) to prevent a crime or carry out an investigation and (iv) to protect the rights, property or safety of the Processor, its subsidiaries or third parties.

The Customer's Personal Data may be transferred outside the European Union. When the Processor transfers Personal Data, it signs Standard Contractual Clauses with its Subprocessors, as laid down by the European Commission.

The Service Provider has appointed a Data Protection Officer ("**DPO**") whose contact details are as follows : dpo@sinari.com

Data subjects have a right of access, rectification, erasure and portability of their Personal Data. They may also request that the Processing of this Personal Data be restricted or object to its Processing under the conditions laid down by the Laws and Regulations on data protection. Lastly, they may inform the Processor of their instructions regarding the fate of their Personal Data in the event of their death when the contract is governed by French Law.

If the Customer considers that the Processor is not complying with its legal obligations with regard to the protection of Personal Data or that it has not responded effectively to the Customer's request, the Customer always has the right to lodge a complaint with the competent supervisory authority.

The Processor implements organizational and technical measures to guarantee the security and confidentiality of the Data it processes.

The Processor only keeps the Personal Data of the Data Subjects for as long as is necessary for the operations for which it was collected and in compliance with the regulations in force. Generally speaking, the Personal Data processed by the Processor under the Contract is kept for the duration of the commercial relationship and then deleted. Certain Personal Data may be kept in intermediary storage following the end of the business relationship, in accordance with the legal obligations to which the Processor is subject (e.g. storage of accounting documents), or because this Personal

Data is of legitimate administrative interest to the Processor (e.g. retention for evidence purposes for the statute limitation periods).

9 Responsibilities

Any person who has suffered material or non-material damage as a result of a breach of the Data Protection Laws and Regulations has the right to obtain compensation from the Controller or the Processor for the damage suffered in its entirety.

Where the Controller and the Processor are involved in the same Processing and are responsible for a damage caused by the Processing, the Controller or the Processor shall be held liable for the damage in its entirety. In this case, the Party who has completely repaired the damage suffered is entitled to claim from the other Party that part of the reparation corresponding to its share of responsibility for the damage.

The Processor shall only be liable for the damage caused by the Processor if it has failed to comply with this contract, in particular where it has acted outside or contrary to the lawful instructions of the Controller, and/or if it has failed to comply with the obligations laid down by or pursuant to the applicable data protection regulations, without prejudice to its liability under other rules.

The Processor shall be exonerated or may limit its liability if it proves that it is not responsible for the event which caused the damage. However, the Processor may not invoke a breach by a Subprocessor of its obligations under this contract to escape its own liability. In other words, the Processor is liable to the Controller for the poor performance of the contractual obligations of its own Subprocessors.

10 Term and termination

This contract is concluded for an indefinite period.

It comes into force on the date on which the Main Contract is signed. Either Party may also terminate the contract by giving notice of this decision by registered letter, subject to a notice period of one (1) month.

If, for any reason whatsoever, the Processor is unable to fulfil its obligations under this contract, it undertakes to inform the Controller immediately, in which case the latter will have the right to ask the Processor to suspend the Data Processing carried out on its behalf and/or to terminate the contract.

This contract is concluded taking into consideration the person of the Data Processor. As a result, the Processor does not have the right to assign and/or transfer this contract and/or the rights and obligations arising from it to one or more third parties without the prior written consent of the Data Controller.

11 Nullity of a provision

The potential nullity of a provision of this contract shall not affect the validity of the other provisions of the contract. The Parties will make every effort to replace the invalid provision with a valid one.

12 Applicable Law and Competent Jurisdiction

This contract is governed by the national law of the Processor's principal place of business.

Any dispute relating to the interpretation or performance of this contract will be subject to the courts of this national law.