Compliance supporting documents with the new European regulation for the management of personal data

Sphinx and the RGPD: our commitment to the protection of personal data

The General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, contains the most important changes to the EU privacy and data security legislation for residents of the EU over the last 20 years.

It is designed to give EU citizens greater control over their data by strengthening their rights, empowering data processors (process managers and subcontractors), and finally giving credibility to the regulation through enhanced cooperation between the data protection authorities.

As a result, companies that host, collect, process and analyze personal data are given new organizational, technical and legal responsibilities.

What is a personal data exactly ?

Personal data is all the information relating to a natural person (the person concerned) that can be used, online or offline, to directly or indirectly identify the person. It can be a name, a photo, an email address, a phone number, bank details, a postal address, a location data (IP address, GPS data) ...), medical information, ...

There is no distinction between personal data relating to a person in his private, public or professional functions - all are covered by legislation.
Some information are furthermore classified as sensitive data. This concept concerns information relating to racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life or the details of criminal offenses.

The use of these data is framed even more strictly by the regulation. The processing of such data with Sphinx software is to be done anonymously.

How does Sphinx ensure compliance ?

At Sphinx, we have made personal data and data security a priority, and we have dedicated significant resources to comply with this new regulation. Here are some of the steps we have taken to prepare for the coming into force of the GDPR :

As a first step, we have had an audit conducted by an independent firm to verify the measures to be implemented to comply with the new obligations. The audit focused on organizational, technical, and legal aspects. This allowed us to take the necessary actions to comply with the new regulations, namely:

- Designation of a DPO
- Formalization of our personal data protection policy
- Establishment of a register of treatments for our subcontractor activity

- Modification of the general conditions of sale by contractualizing our commitments in terms of protection of personal data
- Modification of SphinxOnline applications for the management of user passwords
- Modification of the TOS (available from June 15, 2018)
- Training and raising awareness of internal teams on the protection of personal data.

The purpose of this document is to provide our clients with all the documents necessary to comply with GDPR.

Personal data protection policy

Table of content

1 Introduction

1.1 Object

This document stands for the policy of protecting personal data of Sphinx Development subcontractor as part of the General Regulations of the Protection of Personal Data.

1.2 Responsibilities

The DPO is responsible for managing the reviews of this document.
This policy is reviewed at least once a year.
A review must be performed in the following cases: regulatory changes, exceptional events, major changes or incidents.
Any new version of this document is approved by the DPO.

1.3 Classification

This document is public. It is available to all Le Sphinx Developpement customers.

2 FAD Protection Policy

2.1 Application field

This policy of protection of personal data applies for the handlings between Le Sphinx Development and its customers in the framework of the supply of Declic, SPHINX IQ2, SphinxOnline, DATAVIV' solutions (The Sphinx Development, subcontractor in the sense of the RGDP). All collection and processing of personal data is done by the Customer, named in the document "controller".

2.2 Collection of FADs

2.2.1 SPHINX IQ 2

The personal data of the persons concerned are collected under the responsibility of the **controller**.
Within the software, connection logs contain IP addresses, ports, and referrers.

2.2.2 SphinxOnline, DECLIC & DATAVIV'

The personal data of the persons concerned are collected under the responsibility of the **controller**.
Within the software, connection logs contain IP addresses, ports, and referrers.

2.3 Purposes of DCP treatments

2.3.1 SPHINX IQ 2

The purpose of treatment of SPHINX IQ 2 is to create, administer questionnaires, and analyze the data provided, in order to communicate results in the form of reports and / or indicators.

2.3.2 SphinxOnline, DECLIC & DATAVIV'

The main purpose of processing SphinxOnline is to access online questionnaires and manage them.
The specific purposes of the treatments performed by Le Sphinx développement are:

- The design of the questionnaires and their formatting
- Dissemination of questionnaires, by e-mail or SMS
- Monitoring and analysis of results in real time,
- Hosting on SphinxOnline servers.

2.3.3 SPHINX technical support

The purpose of the technical assistance activity is to provide support to customers and to resolve requests sent by customers via a ticket.
To this end, they have access to customer accounts, and all the information contained in the questionnaires in the SPHINX products, as well as to the associated log files.

2.3.4 Sphinx Institute

The aims of the Sphinx Institute activity are to carry out for the customers:

- The definition of the methodology and the development of the survey support
- Dissemination of studies on different media
- Rigorous analysis to guide decisions
- Setting up collaborative sharing platforms

For this purpose, Sphinx employees who are members of the Research Department have access to the questionnaire data and the data provided by the client during the service. They use LE SPHINX DEVELOPPEMENT solutions in order to achieve the desired goals.

2.4 Transmission of FADs

Transfers outside the EU if they exist are under the responsibility of the controller.

2.5 FAD rights exercises

In accordance with Chapter 3 of the Regulations, the person concerned by the FAD may exercise his rights as provided for in Articles 12 to 23.
The DPO of Le Sphinx Développement's client is the person who receives the request for the exercise of the rights.
The Sphinx Development provides the functionalities allowing the exercise of these rights.
If necessary, the DPO of Le Sphinx Développement is the point of contact of the customer's DPO.
The DPO of Le Sphinx Développement can be contacted by email at dpo@lesphinx.eu

2.6 Conservation of FADs

All data collected by the controller are saved locally by Le Sphinx Développement on each server and replicated to a remote server. The shelf life of backups by Le Sphinx Développement is for a period of 6 months. The retention period for data outside this backup use, is under the responsibility of the controller depending on the personal data that are retrieved from the questionnaires.

2.7 Safety measures on FADs

The Sphinx Development protects personal data by setting up physical and logical security measures to protect personal data from unauthorized access, misuse, disclosure, loss and destruction.

2.7.1 SPHINX IQ 2

- ENCRYPTION
  - Personal access account passwords for SPHINX IQ 2 software are encrypted.
  - Surveys can be encrypted.

2.7.2 SphinxOnline, DECLIC & DATAVIV'

- ENCRYPTION
  - Passwords for personal SPHINX online access accounts are encrypted (HASH PBKDF2).
- LOGIC ACCESS CONTROL
  - The accesses are made by login / password.
  - All accounts are nominative (login / password).
  - Server backups are replicated to other sites and access is restricted.
  - Restriction of IP and a VPN connection on the servers.
- SERVERS PHYSICAL ACCESS CONTROLLING
  - The servers are hosted in the Datacenter of the OVH company, on the Roubaix site and maintained by Ergole Informatique, an exclusive subcontractor of Le Sphinx Développement for the operation of hosted services.
  - Access to hosted servers is restricted.
- LOGGING
  - Connection logs containing IP addresses, ports, and referrers are kept and maintained.

3 LE SPHINX DEVELOPPEMENT DPO Contact

The main mission of a DPO is to ensure that the organism that has designated him/her is in compliance with the legal framework for personal data. The function of Data Protection Officer is a key element of co-regulation, by practice.

This objective is achieved through the following missions:

- Informing and raising awareness, spreading a "Data Protection" culture
- Ensure compliance with the legal framework
- Inform and empower, alert if necessary, his/her controller
- Analyze, investigate, audit, control
- Establish and maintain documentation for Accountability
- Mediate with the people concerned
- Submit an annual report to his/her controller
- Interact with the supervisory authority

The DPO of Le Sphinx Développement can be contacted by email at dpo@lesphinx.eu

Modification of the general conditions of sale

Article 9: PROTECTION OF PERSONAL DATA

9.1 Personal Data processed in connection with the use of the Solution

In the meaning of Law No. 78-17 of January 6, 1978 amended "Data Protection Act" and Regulation (EU) No. 2016/679 called "General Data Protection Regulation" (together "Applicable Law"). Protection of Personal Data "), the Customer is the person in charge of the processing of Personal Data carried out in connection with the use of the Solution by the Users. As such, the Customer undertakes to implement appropriate technical and organizational measures to ensure and be able to demonstrate that the processing performed is in accordance with the **Law Applicable to the Protection of Personal Data**.

In application of the Contract, the Publisher may be required to process Personal Data on behalf of the Client and on the instructions of the latter. As such, he acts as subcontractor of the Customer and is responsible to him/her for the respect of the requirements of the Law Applicable to the Protection of Personal Data. Consequently, the Publisher commits to respecting the following obligations and to have them respected by his staff:

- To treat the Personal Data in the strict and necessary framework of the Services agreed between the Parties under the Contract and to act only on the basis of the documented instructions of the Customer;

- Ensure the confidentiality of Personal Data and ensure that each person authorized to process such data undertakes to respect confidentiality or is subject to an appropriate confidentiality obligation;

- Ensure the security and integrity of the Personal Data. As such, the Publisher implements and maintains appropriate security measures of its information system, in accordance with the requirements of the Law Applicable to the Protection of Data. These measures aim to (i) protect the Personal Data against their destruction, loss, alteration, disclosure to unauthorized third parties, (ii) ensure the reinstatement of the availability of Personal Data and access to it in a timely manner in the event of a physical or technical incident;

- Not to use the Personal Data for purposes other than those provided for in the Contract and strictly related to the performance of the Services agreed between the Parties, and not to retain them beyond the duration of the Agreement or any other period specified by the Client. In any case, the Publisher undertakes to delete and destroy any copy or return to the Customer any Personal Data at the end of the Agreement, except for a copy kept by the Publisher for the purpose of proof of the good performance of its contractual obligations;

- Not to give, rent, assign or otherwise communicate to any other person, all or part of the Personal Data;

- Not to subcontract the performance of the Services that involves the processing, in whole or in part, of Personal Data, without the prior written consent of the

Customer. Without prejudice to the foregoing, the Client acknowledges and agrees that the Publisher subcontracts (i) the development and maintenance of the Solution to ERGOLE Informatique (RCS Grenoble 408 088 433) and (ii) the hosting of the Solution by the company OVH (RCS Lille Métropole 424 761 419).
The Publisher guarantees that any subcontractor that is presented to the Client offers sufficient guarantees as to the implementation of appropriate technical and organizational measures so that the processing meets the requirements of the Law Applicable to the Protection of Personal Data, and guarantee the protection of the rights of the persons concerned;

- Provide assistance to the Customer to enable him/her to respond to any request for the exercise of a right, request or complaint of a person concerned, within the deadlines and in accordance with the conditions provided by the Law Applicable to the Protection of Personal Data or a data protection authority or other regulator;

- To assist the Customer in carrying out privacy impact assessments and / or as part of formalities to be performed by the Client. The Customer acknowledges and agrees that the provision of assistance to be performed in this context will be the subject of a separate service proposal from the Publisher;

- Make available to the Customer, subject to compliance with a confidentiality agreement, all the information necessary to demonstrate compliance with the obligations provided for in this article and to enable audits to be carried out, including inspections, by the Customer or any auditor appointed by him/her and contribute to these audits;

- Not to transfer Personal Data processed under the Contract to countries outside the European Economic Area that have not been recognized by the European Commission as providing an adequate level of protection (i) without first obtaining the express written authorization of the Client and (ii) without the establishment of legal instruments recognized as appropriate by the Law Applicable to the Protection of Personal Data to supervise the transfer (s) concerned.

The Publisher undertakes to immediately alert the Client in the event of a breach of the Personal Data and to assist it in the implementation of any action to deal with this data breach, including notifications to the competent authorities and persons concerned by the deficiencies and to provide any useful information allowing to assess the extent of the violation of Personal Data and to identify the means to its remedy.

9.2 Personal Data of the Customer and Users

The supply of the Services and, more generally, the proper performance of the Contract implies the collection, by the Publisher, of the Personal Data of the Customer and the Users.

The Client acknowledges and agrees that the Publisher may use the Personal Data of the Customer and Users for marketing and promotional information on the Solution and / or other products and services of the Publisher.

The Publisher implements and maintains appropriate security measures of its information system in order to protect the confidentiality of Personal Data, in accordance with the requirements of the Law Applicable to the Protection of Data.

The Publisher agrees not to assign, rent or transmit the Personal Data of the Client and Users to third parties other than the server host and the developer of the Solution as mentioned in article 9.1 above, except legal or judicial obligation to do so.

In accordance with the Law Applicable to the Protection of Personal Data, the Customer and the Users have a right of access, rectification, limitation, deletion and portability of the Personal Data concerning them. The Client and the Users also have the right to oppose, for legitimate reasons, that their Personal Data is subject to processing. These rights can be exercised at any time from the Publisher by email at the following address: dpo@lesphinx.eu

Modification of SphinxOnline, Declic and DATAVIV' applications for password management

New authentication system when updating servers as of May 28, 2018

In order to comply with the new regulations on the management of personal data and to comply with best practices on the security of information systems, we have upgraded our authentication system to SphinxOnline, Declic and DATAVIV 'applications and have reinforced the password management policy.

From now on, the initialization of the password linked to an account is the responsibility of the user of the application. This password is encrypted irreversibly. It is known only by the owner of the account.
Our technical support and our hosted services operating service are no longer able to recover it. In case of forgetfulness, it is necessary to reset it.

1. **Strengthening the password policy**

As soon as your account is created, the SphinxOnline account manager, Declic or DATAVIV' receives an e-mail inviting him/her to create his password. It connects to a secure URL from which it enters the password of its choice respecting the constraints necessary to secure your information (8 characters minimum, at least 5 different characters, at least one lowercase, at least one number, at least one special character). He is the only person who knows his password.

The passwords must be renewed every 6 months and must be different from the 5 previous passwords.

To avoid fraudulent access attempts, logging into an account is not possible for a period of 5 minutes after 5 unsuccessful attempts.

2. **Dual factor authentication**

To further enhance the security of access to our applications, dual factor authentication is available. This allows the user to protect access to the account with a second one-time code generated by a third-party application.

3. **Traceability of access and connection log**

To provide better visibility into your account activity and operations, logging behavior has been improved to more accurately track all changes and accesses made.