Data Management Plan

Deliverable 1.1

31 March 2019

WP Participants:
EURORDIS

V1	27 February	EURORDIS
V2	29 March	ISINNOVA
Final version	31 March	All partners

The Rare2030 project is co-funded by the European Union Pilot Projects and Preparatory Actions Programme (2014- 2020). This leaflet is part of the pilot project PP-1-2-2018-Rare 2030. The content represents the views of the author only and is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission or any other body of the European Union.

Contents

Purpose of Rare 2030 Management Plan

The purpose of the Data Management Plan (DMP) is to provide an analysis of the main elements of the data management policy that will be used throughout the Rare2030 project with regard to all the datasets that will be generated by the project.

This document will evolve with the lifespan of the project and will be reviewed at M6, 12, 18 and 24.

Five principle data sets will be used throughout the Rare 2030 project:

1. KOL interviews
2. Input from the Panel of Experts
3. Orphan Drug Data
4. Survey responses from the Rare Barometer Voices Survey Platform (RBV Survey)
5. Survey responses from European Reference Network Health Care Professionals and Coordinators (ERN and HCP Survey

1. KOL Interviews

Approximately 10 face-to-face or telephone interviews will be conducted by ISINNOVA starting in M5 or the project. These interviews will allow experts to provide WP4 participants with novel and objective insights beyond the common trends for rare disease policy. The interviewees will be selected among high-level representatives of key actors involved in health systems with a wide perspective over its dynamics. The active participation of EURORDIS and all project partners will greatly facilitate the identification and recruitment of interviewees. Responses during the interview will be recorded with the permission of the interviewee for reference. Responses from the 10+ interviews will be analysed as a deliverable in WP4. ISINNOVA will produce synthesis of existing insights on trends, disruptive events, wild cards and weak signals of external driving forces likely to influence Rare Disease care and governance now and in the future based on these interviews at which time and recordings will be destroyed. No explicit quotes from the interviews will be used unless consented by the KOL.

2. Input from the Panel of Experts

Panel of Experts participants will be regularly consulted for their input during the project. All input will be summarized collectively with not association of opinions with names. The membership list of Panelists will be published on the website.

3. Orphan Drug Data

The Imperial College of London team plans provide a snapshot, supported by in-depth analysis, of a specific aspect of rare disease policy – the development and market launch of therapies for rare diseases or orphan drugs. To do this the team will collect data from different sources, namely:

- Historical data on R&D: to be provided by IQVIA R&D Pipeline platform
- Market data (prices and quantities per drug/ATC): we are currently assessing the feasibility of buying these data from IQVIA.

- Burden of disease data, prevalence and incidence data: to be collected from different sources including, for example, the IHME GBD study.
- Country level data from the World Bank and similar sources on potential confounders of innovation and market launches.
- Firm level data if feasible.
- Policy and regulatory data that can shape innovation and market launches including financing and reimbursement policies, market access incentives and regulations, policies targeting rare diseases and orphan drugs, etc.

Several applied micro econometrics tools will be used for the analyses. Data will be stored on an encrypted drive. Data is at drug/innovation level and therefore does not contain any sensitive fields. ICL is bound. We are bound by the terms of any executed Data Access Agreement between Imperial College London and the Data Provider, meaning that R&D and market data obtained from IQVIA will not be shared. The other datasets are freely available online. In line with Imperial College London data preservation guidelines we will preserve all data supporting published research conclusions at Imperial for at least 10 years from the end of the project that produced it.

4. Survey responses from the Rare Barometer Voices Survey Platform

Rare Barometer Voices is a EURORDIS initiative that aims to make the voice of rare disease patients stronger. The objective is to transform your opinions and experiences about topics that directly affect them into figures and facts that can be shared with a wider public. This platform will be used to identify preferred scenarios in the Rare2030 project with the patient community and request information on how these preferred scenarios affect their lives and should be reflected in rare disease policy.

Rare Barometer Voices participants provide their email address during registration and give explicit consent to participate on a regular basis in online surveys. They also have the possibility to unsubscribe from the programme. When re-contacting participants, contacts details are replaced by an automatically-generated key. The final, stored electronic records contain no identification of the participating respondents and responses can only be analysed as overall or grouped data.

The programme has been approved by the French data protection authority (CNIL).The survey software used by the programme (Sphinx software) stores the data in France, thus respecting the high European data protection standards. The Security framework of the software

Confidentiality rules of the website are available here (**https://www.eurordis.org/voices#confidentiality**) and include the following:

- All of the information shared with EURORDIS through the RBV platform is **completely confidential and anonymous**, it is used to create a collective analysis and personal information will not be shared with anyone other than the Project Leader.
- Encryption systems prevent the link between registration details and responses in a survey.
- This programme is owned independently by EURORDIS and is a non-profit initiative; no commercial use of details will be made at any time.
- This programme is approved by the CNIL (Commission nationale de l'informatique et des libertés, French data protection authority).

- The data is stored by Le Sphinx (a software company) in Grenoble, France, where they maintain a protected environment to ensure the secure storage of data. Le Sphinx is an online security platform with 24-hour surveillance and access control that has worked with many non-profit clients in the past.
- Answers are used for research purposes only. They will never be stored or used for purposes other than those indicated in the participation instructions.
- You can unsubscribe at any time by clicking the unsubscribe link in the survey email. If you decide to unsubscribe from Rare Barometer Voices your data will not be kept, it will be destroyed.

The security framework of the Software is included in Annex 1.

No individual data will be shared to protect the potential identification of patient respondents (as they are affected sometimes by very rare diseases). Only global statistics will be published and shared with Rare 2030 partners and external parties.

5. Survey responses from European Reference Network Health Care Professionals and Coordinators

A similar survey will be conducted with the 900+ healthcare professionals affiliated with the 24 European Reference Networks. As the platform and methodology for this data collection exercise have not yet been defined – this portion of the Data Management Plan will require and update anticipated at month 6.

Annex 1 (in French)

Security statement

SphinxOnline 4.14

Last update : 24/05/2018

Table of content

1 Introduction

For more than 30 years, Sphinx Développement has been publishing and distributing software solutions dedicated to the survey and data analysis. For more than 15 years now, Le Sphinx has been offering hosted services to enable its customers to carry out online survey projects independently. A set of applications is thus accessible directly via the Internet to allow setting the questionnaires, to diffuse the surveys, to host all the data collected and to share results in the form of interactive reports.
Therefore, securing access to this data has become one of our main concerns and we strive to ensure our customers maximum service availability and total protection of their surveys.
The purpose of this document is to list and describe all the measures taken and the arrangements put in place to meet this objective.

2 Infrastructure

2.1 Hosting

The servers are hosted in the Datacenter of the company OVH which ensures the physical security. The data are stored in Roubaix and Strasbourg in France.
The provision and operation of infrastructures (datacenter, servers, networks) provided by OVH is certified ISO 27001: 20013 (Roubaix) and ISO 270001: 2005 (Strasbourg).
Outsourcing servers is provided by our services. Our host does not have access to the data stored on our servers.

2.2 Network and communication protocols

The production servers are isolated in a DMZ and are protected against intrusions by a network firewall.
The DMZ zone is only accessible over the TCP protocol on ports 80 and 443.
Flows arriving on port 80 (http) are automatically redirected to port 443 (https).

OVH incorporates a mitigation solution that protects the infrastructure from a massive denial of service attack without blocking legitimate flows.

All data exchanged between the client software (web browser or Sphinx IQ / IQ2) and the servers are encrypted via the TLS protocol.

SSL is disabled. TLS versions 1.1 and above are prioritized, and TLS 1.0 can be accepted if the user's browser does not support higher versions.

Certificates are generated from 2048-bit key and signed with the sha256 algorithm.

2.3 Systems security

Access to the servers is restricted to operating service personnel (<8 people) and is done through a VPN connection (IPsec tunnel or SSL with double factor authentication).

Domain administrator access, physical machine administrator, and virtual machine administrator are separate.

The passwords of these administrators adhere to the following policy and must:

- have at least one number, one lowercase, one uppercase letter, one special character
- to be different from the previous 24 passwords
- be changed every 6 months

After 5 unsuccessful access attempts, account authentication is not possible for 60 minutes.

The local administrator passwords for each machine are changed to passwords that are at least 22 characters long and include at least one digit, one lowercase, one uppercase letter, and one special character.

2.4 Anti-virus protection

Software anti-virus protection is installed on all servers. The administration of this one is centralized. Alerts are reported in real time and protection is checked daily.
Strategies in places include:

- a complete analysis every week
- real-time protection
- a daily update of the signature database

2.5 Safety of sensitive workstations

The sensitive workstations (developers, administrators, support service, ...) are protected by password, the disks are encrypted (bitlocker) the lock of the computer is automatic after 10 minutes of inactivity.

All workstations benefit from virus protection.

2.6 Availability

An availability rate for Sphinx servers is guaranteed at 99.9% over 365 days.
This rate does not take into account interruptions related to scheduled maintenance.
These take place 1 to 2 times per month on average between 3:00 am and 4:00 am (UTC + 1). If they are to be carried out outside this time slot, the details of the intervention are communicated to the owners of the accounts or to the person responsible for the administration thereof within a period of two weeks.

2.7 Continuity of services

Service continuity devices are described in the service continuity plan.
This document is confidential but it covers the following points:

- Background and infrastructure
- Diagnostic aid and intervention thresholds
- Failure scenarios
- Loss of Network Connectivity: Vrack, VLAN configuration, ...
- Physical server hardware failure: Host, domain controller, backup server
- The failure of the virtual machine performing the role of firewall or loss of its configuration

In the event of a server failure, the service will be re-established on another machine within a maximum of 8 hours after notification of the failure.
The maximum data loss is 24 hours

Since the servers are currently hosted by the company OVH (https://www.ovh.com), the continuity of SPHINX services is therefore subject to that of the internet access provided by OVH. In case of interruption of this service, for any reason whatsoever, SPHINX DEVELOPPEMENT undertakes to do its utmost to find a new supplier.

The data is stored on RAID 5 or Raid 50 disk groups. A monitoring system can alert our teams in the event of a disk failure

2.8 Surveillance

The applications, the systems and the network are monitored 24 hours a day, 7 days a week. Remote access tests to applications are performed internationally by INTERNETVISTA (www.internetvista.com).

Our teams intervene from 8am to 11pm, 7 days a week in the event of alert raised by the various tools of monitoring.

2.9 Backup Management

The data is saved daily and is kept for a maximum of 6 months.
They can be retrieved on request until 2 months after the expiration of the subscription.
These backups are encrypted via the AES (256-bit) algorithm.

The backup data are replicated between the info center of Roubaix and Strasbourg.

2.10 Update Management

Upgrades of the operating systems are made within a maximum of 7 days after the patches are made available. Approval of updates is done manually (WSUS features).

3 SphinxOnline Solution

3.1 Access protection

The security of the user accounts is ensured by login / password.
Passwords are stored on servers in a non-reversible encrypted manner (HASH PBKDF2 HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 iterations)

Passwords must meet certain minimum complexity requirements (8 alphanumeric characters and special characters) and must be changed to a minimum every 6 months.
The last 5 passwords cannot be reused.
After 5 unsuccessful access attempts, the account login is blocked for 5 minutes.

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.

Access to surveys and / or add-ons can also be password protected.

3.2 Incident management

The technical support service is available at 04 50 69 82 98 from Monday to Thursday from 8:30 am to 12:30 pm and from 2 pm to 6 pm and Friday from 8:30 to 12:30 and from 14h to 17h (Paris time).

The response times for performing a corrective update depend on the type of anomaly:

Type of anomaly	definition	Correction time
Blocking	Refers to any anomaly that makes it impossible to use a feature without a workaround.	Within 8 working hours
Major	Refers to any anomaly involving degraded operation of at least one feature.	Within 72 working hours
Minor	Refers to any anomaly that has a workaround, without degrading the overall operation.	Made available during minor updates

The correction time starts at the discovery of the problem.

3.3 Interchange security

When publishing or importing a survey from the Sphinx IQ / IQ2 software, the files exchanged between the server and the software are stored in an encrypted archive (128-bit AES algorithm).
The file exchange is performed only after verification of the login / password of the user.

3.4 Portability of the data

It is possible to export survey data, email campaigns or SMS in different standard formats like .csv or .xls

3.5 Traceability

Queries and connections are logged in application event logs. These logs record all the connections, recordings, modifications, navigation actions of the respondents, ...
These logs are kept for a period of one year then are automatically deleted

3.6 Cookies

The SphinxOnline solution uses only technical cookies necessary for the proper functioning of the applications for the following purposes:

- Security guarantee: authentication, access control, ...
- Preferences: Choice of language, current working directory, display options, ...

These cookies are not communicated to any third party and are not exploited for advertising or targeting purposes.

4 Administrative and organizational security

4.1 Management of security vulnerabilities

SPHINX DEVELOPPEMENT is held to an obligation of means to ensure the integrity of the network and systems against any act of external malicious or known cyber-attack.

In the event of an attempt or suspicion of breach of information security or theft of personal data. We undertake to notify the owner of the account within 8 business hours from the discovery of the problem.

Our teams monitor daily the alerts issued by CERT-FR and, when necessary, take the appropriate measures to guard against the vulnerabilities mentioned in these alerts, which may involve the application of corrective measures or the implementation of recommendations.

4.2 Control and monitoring measures

A configuration audit and intrusion tests on the solution are performed each year by an external firm specializing in computer security. In 2018, the firm Oppida was mandated;
The summary of the counter audit report will be available in the course of July 2018.

Any critical faults reported during these audits are corrected as soon as possible.

An internal document lists all possible improvements in terms of security.
Each element of this document categorized according to several criteria (exploitability, difficulty of implementation, criticality, probability ...). A monthly review of this document is performed to update the elements with regard to the state of the art in terms of safety and to define future actions.

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.