



# Service booklet

**Cegid Wittyfit**

February 2023 version

**cegid**

**CONTENTS**

**Table of contents**

Table of contents

Preamble.....3

Our infrastructure .....3

    Technical architecture.....3

    Managing data confidentiality and account pseudonymization .....4

    Connection modes .....6

    A fully responsive solution (tablet, smartphone, desktop).....6

    RGPD / CGU / identification management and personal data processing.....7

Security-oriented hosting .....9

    High-quality secure hosting.....9

    Network infrastructure .....9

    Backup service.....10

    Security audit .....10

Our service level agreements (SLA) .....10

RGPD .....13

    Preamble .....13

    Warranty .....13

    Subcontractor's obligations.....14

    Security .....15

    Data breaches .....16

    Keeping the register .....16

    Data retention.....16

    Mapping personal data processing .....17

## Preamble

The purpose of this document is to provide an overview of our hosting, security and commitment services. Each of these elements can be expanded upon at the request of our customers.

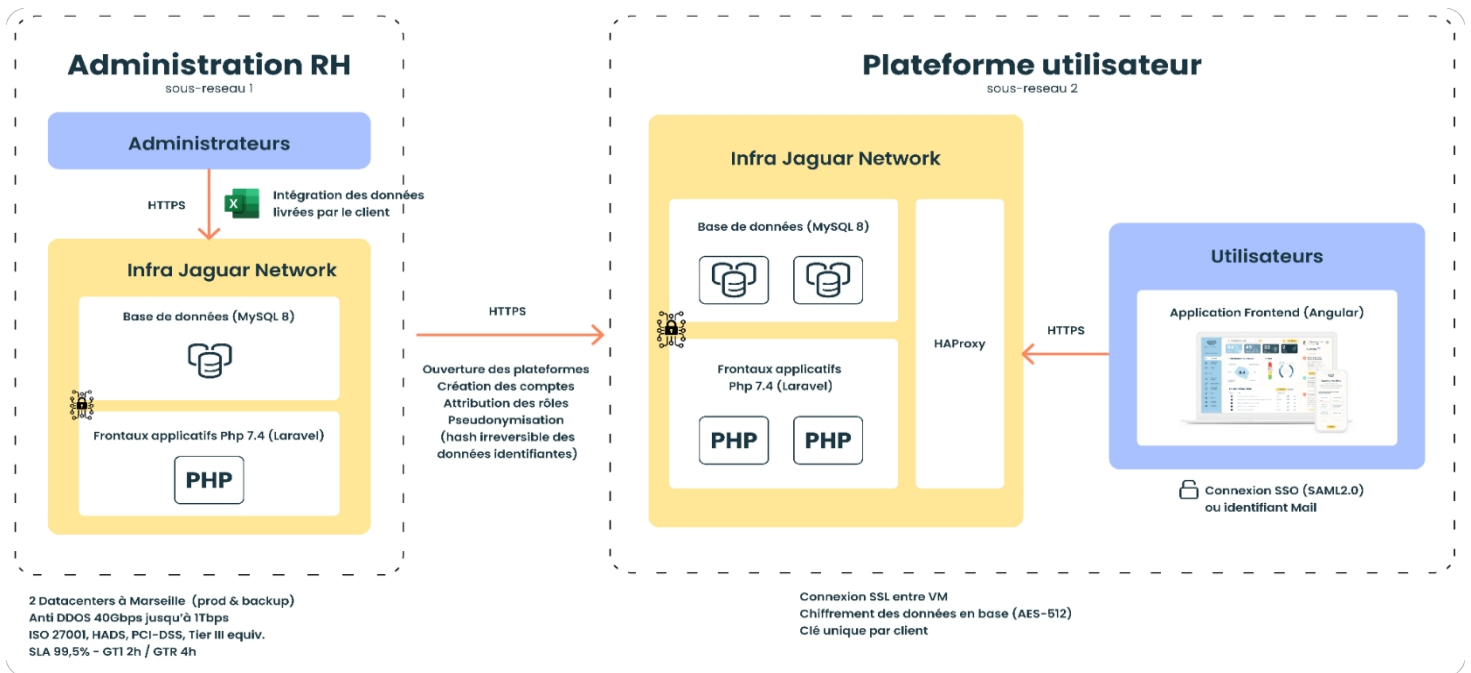
## Our infrastructure

### Technical architecture

Our infrastructure is hosted by Jaguar Network, comprising 2 watertight sub-networks, one for HR administration and the other for the Cegid WITTYFIT application and its technical administration. Our solution runs on a LAMP environment

It is structured as follows:

- at least 2 PHP 7.4 application front-ends (Laravel)
- Databases (MySQL 8, Redis) isolated/client (possibility of instantiating a dedicated server)
- Web application based on Angular 9+, accessible only via HTTPS
- Nightly 2-hour backups + Weekly server image



HAProxy enables us to set up specific redirection rules to comply with customer requirements (e.g. IP restriction), or internal organization. Application front-ends are virtualized, and a load-balancer system ensures that we can cope with occasional peaks in usage, while the host can rapidly set up new instances in the event of a longer ramp-up.

### Managing data confidentiality and account pseudonymization

The confidentiality of our users' data is one of the key factors in our employees' commitment to the tool, and consequently to the overall approach. Cegid Wittyfit has integrated data protection right from the product's design and from its very first lines of code. Thus, in line with the RGPD and the logic of "accountability", Cegid Wittyfit respects "privacy by design".

In addition, in order to be able to work in partnership with the Clermont-Ferrand University Hospital, we had to meet the criteria set by its ethics committee - in addition to those of the RGPD - in terms of data protection. Last but not least, our data is hosted in France by an Authorized Health Data Host (HADS).

Cegid Wittyfit guarantees its users and co-contractors maximum data protection measures. We can of course provide you with all the documents you need to carry out your PIA - Privacy Impact Assessment.

Cegid Wittyfit guarantees user confidentiality during data processing and retrieval.

That's why we've split our application into 2 platforms. One for account management, in the hands of an operator, who uses the list of authorized users to authorize account creation and activate authorizations for each account. This platform (Admin-RH) is separate from the user feedback platform (separate sub-network), and controls account creation after pseudonymization.

When creating accounts :

For the transfer of initial account creation data and role assignment, we provide the customer with a secure, encrypted dropbox (opentrust MFT solution, AES-256 encryption) for data transfer. Encrypted e-mail from the customer can also be used. Temporary storage is in a container encrypted via Veracrypt (AES-512) for the duration of the operation.

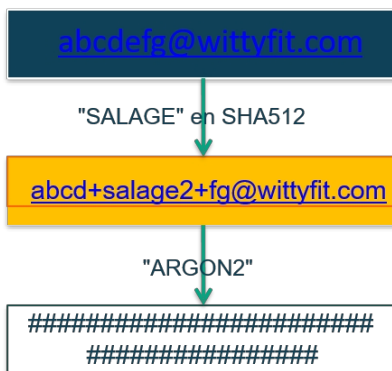
The administration platform is accessible via strong 2-factor authentication with rotation of passwords.

When processing data :

The only identifying data provided by the company is not stored in the database, but is replaced by a non-reversible encryption:

>[abcd@wittyfit.fr](mailto:abcd@wittyfit.fr) + salting then sha512

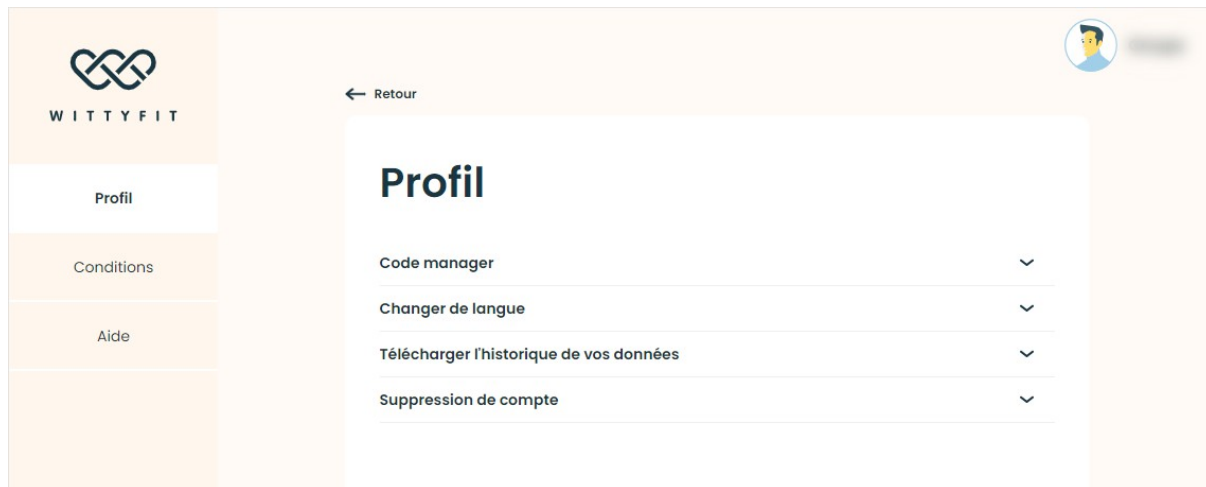
>password + salting2 then argon2



During renditions on our platform :

The results of a group are only displayed if at least 5 people from that group have expressed their opinion. Thus, no data is accessible below 5 respondents. Only users logged in with

their own account can access the data they have entered, either by browsing the various questionnaires, or by requesting a download of the data history from the settings menu.



## Connection modes

There are two ways to connect to the service:

- Mail ID or HR number
- SSO via SAML2

E-mail identifications are secured by the allocation of a unique and temporary verification code before password entry (two-factor authentication). For HR identifiers, the user must define a pair of "secret questions & answers", and can choose to enter a recovery e-mail, and then enter the case of two-factor authentication.

The password policy can be customized by the customer. By default, we ask users to create a password of at least 8 characters, containing at least 3 each of lowercase, uppercase, numeric and special characters. The customer can choose to activate password rotation, and can define the length of time in weeks that a password is valid.

## A fully responsive solution (tablet, smartphone, desktop)

Cegid Wittyfit is available on all digital tools on the market. However, to ensure to ensure perfect deployment of the platform, it will be necessary to validate browsers and devices. main products.



Le mobilité pour  
toucher tous les  
métiers

## RGPD / CGU / identification management and personal data processing

As previously mentioned, as part of its public-private partnership with the CHU de In Clermont Ferrand, Cegid Wittyfit is required to comply not only with the General Data Protection Regulation, but also with the CHU's Comité de Protection des Personnes.

So we meet every one of the safety requirements you mention. Here are just a few of our guarantees:

Hosting of our data at Jaguar Network (Iliad subsidiary) in mainland France (Marseille) with a HADS hosting contract (logs of actions carried out on servers, partitioning of services, access by clearance)

### TOS and user information :

On first connection, the user must read and accept our T&Cs. These are clear, precise and legible. In addition, in order to be able to express themselves via the free fields provided during browsing (ideas, polls), each user must read and accept our "guide to good conduct", which sets out the rules for respecting the confidentiality of company data, and the anonymity of individuals.

Finally, for further protection, short and precise information messages are offered to each user on the means implemented by Cegid Wittyfit to guarantee the confidentiality of responses and data protection. Users are also informed of the purpose of data processing.

Of course, any user can request the deletion of his or her account and all data concerning its identifier.

### Authentication and authorization :

As we have seen, employee e-mails are encrypted (salted and hashed via SHA512), and this encryption is irreversible. In addition, two-factor identification on first connection further enhances user protection.

The date and time of the last connection are displayed on each user's homepage at the time of each new connection, enabling the user to be informed if he or she so wishes.

### Encryption :

User-generated text data is base-encrypted (AES-512). This encryption applies to ideas (title, description, comments), actions (title, description) and free-form survey fields.

### Privacy

None of the questions contain any identifying information.

Results are always aggregated within teams or groups of more than 5 people. This figure is configurable with our customers, but can never be less than 5 respondents.

In the event of insufficient numbers, not only is the group or team result not displayed, but also this is not even calculated or stored in a database.

The same applies when analyzing two antagonistic groups - male/female, for example - if the number of employees in one of the two groups is less than 5, then the other group cannot be displayed either, to avoid inferring results from the total number of employees.

As part of the RGPD, Cegid Wittyfit has set up the position of DPO. Sylvain AKRICHE holds this position and will be your privileged contact: [dataprivacy@cegid.com](mailto:dataprivacy@cegid.com)

We work with major accounts that have enabled us to be certain of total compliance with all RGPD-related rules. If you wish, we can put you directly in touch with our customer contacts, with whom we have been able to test the compliance of all our security parameters.



## Security-oriented hosting

We have entrusted our hosting to Jaguar Network (Iliad Group). As such, Cegid WITTYFIT has subscribed to its Agrément d'Hébergeur de Données de Santé offer, and relies on an Integrated Management System (Quality-Security).



depuis 2010



depuis 2015

Jaguar Network's HADS approval was renewed on [September 2, 2019](#) for a period of 3 years.

### High-quality, secure hosting

Technically, our hosting is as follows:

1. Datacenter Services
  - An Iso 27001 -equiv. Tier3, HDS and PCI-DSS certified datacenter located in France (Marseille) operated by Jaguar-Network for the admin-HR part and for the platform part. The 2 platforms are located on separate sub-networks.
2. Datacenters are served by :
  - High-speed, redundant connectivity,
  - Autonomy from IP operators thanks to management of an AS (Autonomous System)
3. Jaguar Network operates its own 40 Gbps network, including 1 Gbps dedicated to e-Health, extendable to 10 Gbps, with possible support by its ISP up to 1Tbps in the event of a Deny of Service attack.

### Network infrastructure

Our infrastructure breaks down as follows:

1. Cluster Firewalls - Junipers Networks SRX

- Scalable performance for implementing additional services without - any degradation
  - Network segmentation allows administrators to create - security and tailor-made policies
  - 10 Gb/s interfaces to cope with peak loads
  - Comprehensive protection against threats -
2. HAProxy
    - Advanced load balancing (- Load Balancing)
    - Setting up specific redirection rules
    - Performance monitoring and tracking -
    - High availability (clustering)
    - Can be used without an Internet line-

## Backup service

The backup part is orchestrated as follows:

1. commvault & mylvmbbackup backup solutions
  - Ultra-fast restoration of VMs, files and SQL databases
  - Data loss prevention (fast individual backup, snapshot image)
  - Optimized backup performance
  - Checking protection with SureBackup and SureReplica
  - Retention 7j
2. A standard 12-month policy
  - Possibility of adapting the policy as needed (depending on the obligations you or if there is no health data)
3. Localized backups on remote sites
  - Redundant production site in Marseille (on 2 sites)
  - LY003 site (Lyon 69) for the platform section

## Security audit

We carry out annual security tests with Orange CyberDéfense. In the form of vulnerability and intrusion tests, we make every effort to correct vulnerabilities according to their criticality, and we undertake to provide the counter-audit report on request. What's more, our hosting provider proactively follows up and corrects any vulnerabilities reported on its components.

## Our service level agreements (SLAs)

Our technical SLA commitments are summarized in the following table:

Availability level	
Total monthly availability excluding planned downtime	99.5%
Service Desk availability	Working days / Working hours 9 a.m. - 6 p.m.
Maximum downtime for annual maintenance	4H / month maximum
Guaranteed response time (GTI)	2H
Guaranteed recovery time (GTR)	24H
On-call duty	Included
Operating hours	Working days / Working hours 9 a.m. - 6 p.m.

Our operational SLA commitments are summarized below:

A telephone support service to deal with faults is available from Monday to Friday inclusive, from 9am to 6pm. Anomaly reports must be confirmed by email to the Service Provider without delay. The Service Provider will diagnose the fault and then take steps to correct it.

(a) In the event of a blocking anomaly, the report is taken into account within 2 working hours. The Service Provider endeavors to correct the blocking anomaly as quickly as possible, and proposes a workaround solution.

(b) In the event of a semi-blocking anomaly, the report is processed within 8 hours working.

The Service Provider endeavours to correct the fault, and proposes a workaround solution that may allow the use of the functionalities in question within 3 working days.

(c) In the event of a minor anomaly, the report is taken into account as quickly as possible, and the correction of the minor anomaly is proposed in a new version of the Application Service to be delivered as part of the upgrade maintenance.

Our online support platform can handle all of the following operations:


Support Wittyfit / Support





## Support


Vous ne trouvez pas la réponse à votre question dans notre support, n'hésitez pas à nous contacter.


Que pouvons-nous faire pour vous ?

- 

**Support technique**  
Vous avez besoin d'aide pour vous connecter, répondre aux questionnaires ou pour résoudre un dysfonctionnement ? Sélectionnez cet élément pour demander de l'assistance.
- 

**Créer un bug**  
Parlez-nous des problèmes que vous rencontrez.
- 

**Suggérer une nouvelle fonctionnalité**  
Suggérez-nous votre idée pour une nouvelle fonctionnalité.
- 

**Suggérer une amélioration**  
Vous voyez quelque part des pistes d'améliorations ? Nous sommes à votre écoute.
- 

**Autres questions**  
Vous ne trouvez pas ce que vous recherchez ? Sélectionnez cette option et nous vous apporterons notre aide.

## RGPD

### Preamble

Cegid Wittyfit recognizes the strategic and strictly confidential nature of all data held by the company, provided by the Customer. Consequently, Cegid Wittyfit acknowledges that all data and files communicated are subject to compliance with the regulations applicable in France and in the European Union in the field of personal data protection ("Data Protection Regulations"), including in particular:

- the French Data Protection Act no. 78-17 of January 6, 1978, as amended, and any updates thereto;
- Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, applicable until May 25, 2018;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) repealing Directive 95/46/EC, applicable from 25 May 2018;
- where applicable, the texts adopted within the European Union and local laws that may apply to personal data processed under the Contract;
- texts and decisions issued by supervisory authorities, in particular the Commission Nationale de l'Informatique et des Libertés (CNIL); and
- is a matter of privacy and professional secrecy.

- Cegid Wittyfit is the Customer's subcontractor within the meaning of Article 28 of the General Data Protection Regulation.

- Cegid Wittyfit undertakes to put in place all the necessary procedures to ensure that confidentiality and greater security.

### Warranty

Cegid Wittyfit guarantees the customer's compliance with the legal and regulatory obligations incumbent upon it under the following terms

in particular the French Data Protection Act, and compliance with its obligations under the present appendix.

The Customer will carry out any formalities required by the Data Protection Act with a data control authority and, where applicable, will inform the persons concerned by the processing of personal data.

- The Customer is responsible for the content and nature of the Customer Data: in particular, the Customer guarantees the lawfulness and proportionality of the personal data contained in the Customer Data.
- The Customer, as data controller, warrants to Cegid Wittyfit that the processing of personal data carried out under the Contract complies with the requirements of applicable law and in particular that the personal data has been processed in a manner that

that it has been collected for specified, explicit and legitimate purposes, and that the data subjects have been provided with the relevant information at the time of collection of their personal data.

- The Customer shall document in writing any specific instructions concerning the processing of personal data outsourced to Cegid Wittyfit.

### **Subcontractor's obligations**

Cegid Wittyfit undertakes to take all necessary measures to ensure compliance by itself and its staff of its obligations and in particular to :

- not to process or consult data or files for any purpose other than the performance of its services carries out for the Customer under the terms of this agreement;
- not to process, consult data outside the framework of documented instructions and authorizations received from the Customer, including with regard to transfers of personal data to a third country or to an international organization, unless Cegid Wittyfit is required to do so by virtue of a mandatory provision resulting from Community law or the law of the Member State to which it is subject, namely [In this case, Cegid Wittyfit will inform the Customer of this legal obligation prior to processing the data, unless the law concerned prohibits such information for important reasons of public interest;
- do not insert foreign data in files ;
- take all necessary measures to prevent any misappropriation, malicious or fraudulent use of data and files;
- not to carry out any statistical study on the data or any processing other than that requested by the Customer without the approval of its representatives;
- notify the Customer within a maximum of twenty-four (24) hours of any modification or change that may affect the processing of personal data;
- respond within fourteen (14) working days to any request to exercise a right made by a person concerned to the Customer ;
- inform the Customer within a maximum of twenty-four (24) hours if, in its opinion, an instruction constitutes a violation of data protection regulations. At the Customer's request, Cegid Wittyfit will collaborate in the notification of the CNIL.

Furthermore, Cegid Wittyfit will not :

- consultation or processing of data other than that covered by the present document, even if access to this data is technically possible;

- to disclose, in any form whatsoever, all or part of the data used ;
- to copy or store, in any form or for any purpose whatsoever, all or part of the information or data contained on the media or documents entrusted to it or collected by it in the course of the performance of the present contract, outside the cases covered herein.
- Cegid Wittyfit undertakes to take all necessary measures to ensure that natural persons acting under its authority and having access to personal data do not process such data, unless instructed to do so by the Customer, or unless obliged to do so by a mandatory provision resulting from Community law or the law of a Member State of the European Union applicable to the processing operations covered hereby. Cegid Wittyfit ensures that the persons authorized to process personal data undertake to respect the confidentiality of the data or are subject to an appropriate legal obligation of confidentiality.
- It acknowledges and accepts that it may only act in relation to the processing of data and files to which it may have access in accordance with the present terms and conditions and the Contract.
- As a subcontractor, Cegid Wittyfit :
  - keeps a register of processing activities carried out on behalf of the Customer (in accordance with paragraph 5.6 below);
  - provides the customer with the contact details of its Data Protection Officer or, failing that, the person responsible for data protection in its entity.

## Security

- Cegid Wittyfit undertakes, in accordance with the Data Protection Act, to take all necessary precautions appropriate to the nature of the data and the risks presented by the processing(s), to preserve the security of file data and in particular to prevent any deformation, alteration, damage, accidental or unlawful destruction, loss, disclosure and/or access by unauthorized third parties.
- It implements all appropriate technical and organizational measures to protect personal data, taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks, which vary in probability and severity, to the rights and freedoms of natural persons, in order to guarantee a level of security appropriate to the risk.
- Cegid Wittyfit undertakes to maintain these resources throughout the performance of the Contract and, failing this, to use them for the purposes of the Contract.  
immediately inform the Customer.
- Cegid Wittyfit undertakes, in the event of a change in the means used to ensure the security and confidentiality of data and files, to replace them with means of equal or superior performance. No change may lead to a reduction in the level of security.

## Data breaches

- Cegid Wittyfit undertakes to notify the Customer within 24 hours of becoming aware of any personal data breach: any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.
- This notification must be sent to the person designated as the contact point, by telephone and/or e-mail, and then confirmed by registered letter with acknowledgement of receipt. It must specify the nature and consequences of the data breach, the measures already taken or proposed to remedy it, the persons from whom further information can be obtained, and where possible, an estimate of the number of people likely to be affected by the breach.
- In the event of a data breach, Cegid Wittyfit undertakes to carry out all useful investigations into the breaches of protection rules in order to remedy them as soon as possible and to reduce the impact of such breaches on the persons concerned. Cegid Wittyfit undertakes to inform the Customer of its investigations on a regular basis.
- Cegid Wittyfit undertakes to cooperate actively with The Customer to ensure that they are able to meet their regulatory and contractual obligations. It is the sole responsibility of the Customer, as data controller, to notify the competent supervisory authority and, where applicable, the data subject of the data breach.

## Keeping the register

- Cegid Wittyfit, as a subcontractor, undertakes to keep a register of all categories of activities. processing carried out on behalf of the data controller, in accordance with the provisions of the General Data Protection Regulation. Cegid Wittyfit will provide the Customer with access to the register on request.

## Data retention

- At the end of the contract, Cegid Wittyfit will keep the platform data for 12 months in order to enable users to exercise their rights, unless the customer explicitly requests that the data be destroyed earlier. After this period, and unless otherwise required by Community law or the law of a Member State of the European Union applicable to the processing operations described herein, Cegid Wittyfit undertakes to destroy all manual or computerized files storing the information collected.
- Cegid Wittyfit undertakes to provide the Customer, on first request, with a certificate of deletion of personal data.



## Mapping personal data processing

