INFORMATION FOR SYGNANET.PL USERS

What to know in the beginning

After reading the next few pages you'll know whether you like the way in which Sygnanet.pl serves whistleblowers and facilitates the whistleblowing process.

First of all you should know that Sygnanet.pl is an innovative platform created just for the purpose of serving whistleblowers. It's an irreplaceable tool not only meeting the stringent requirements of the EU Whistleblowign Directive, but also outstanding thanks to the revolutionary approach to security and confidentiality of reports.

Sygnanet.pl offers advanced technologies and incomparable advantage in terms of data security. In the world in which security and confidentiality are priceless, Sygnanet.pl is a true innovation transforming the way of serving whistleblowers.

While other services offer data encryption only after they reach the server, Synganet.pl makes sure your data is encrypted already on your personal device. This unique quality offers significant advantages: it makes interception of reports during their transmission virtually impossible. Thanks to this there isn't a slightest chance that administrators or service's developers could read your confidential information.

It's not just a high level of protection: it's a guarantee that your data is secure at every step of their transmission.

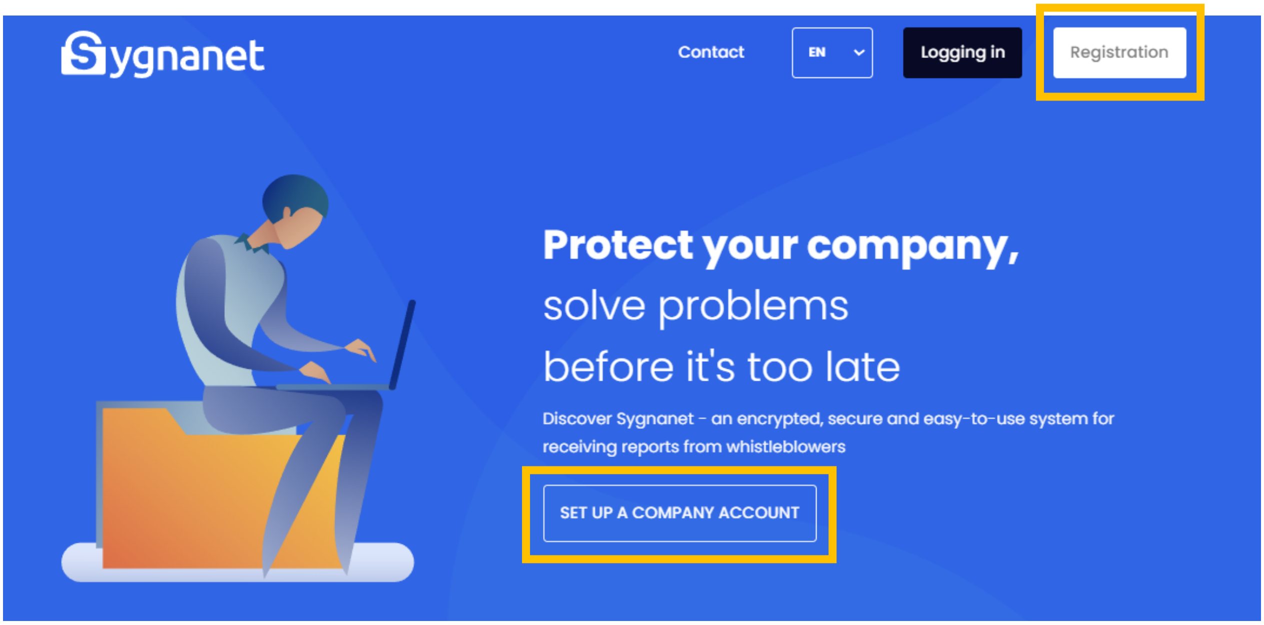
The short guide below will allow you to imagine working with Sygnanet.pl to deal with whistleblowers' reports.

You can find detailed information and how-to videos in the implementation documents of the service.

Let us remind you as well that you can test all of Sygnanet.pl's functions for free by creating a test account for two weeks. No similar service offers such an opportunity.

Setting a web address for the whistleblowers

Using Sygnanet.pl requires registering a person responsible for servicing whistleblowers in the given company and setting a web address for the page with the company's whistleblowers' form.



Protect your company, solve problems before it's too late

Discover Sygnanet – an encrypted, secure and easy-to-use system for receiving reports from whistleblowers

The Recipient of Reports is the person who directly services whistleblowers' reports. **Registering a Recipient of Reports requires entering an email address and a password into the service**. These will be required every time to log in to the service. The first person to register in the service becomes the Principal Recipient of Reports (PRR) and has complete access (that is can access all the reports, process them and manage all the account settings). Other users of the system (other recipients of reports, the administrator and the auditor) may be added afterwards in the Sygnanet panel. The panel is also used to manage their levels of access. While registering, the PRR also sets the **web address** for the with the company's whistleblowers' form. It looks like this:

sygnanet.pl/xxxxx

where xxxxx is a freely chosen string of characters (and the company's identification).

ℹ The overall length of the whole web address cannot exceed 2048 characters. The following characters are allowed: numbers, letters and ( ) ! $ - ' _ * +

The address for entering reports (sygnanet.pl/xxxxxx) should be shared with all the company's employees during an internal training on the reception and servicing of the whistleblowers' reports. The training should also cover the given company's rules concerning servicing of the reports such as the admissibility of anonymous reports, time limits for servicing the reports and so on.

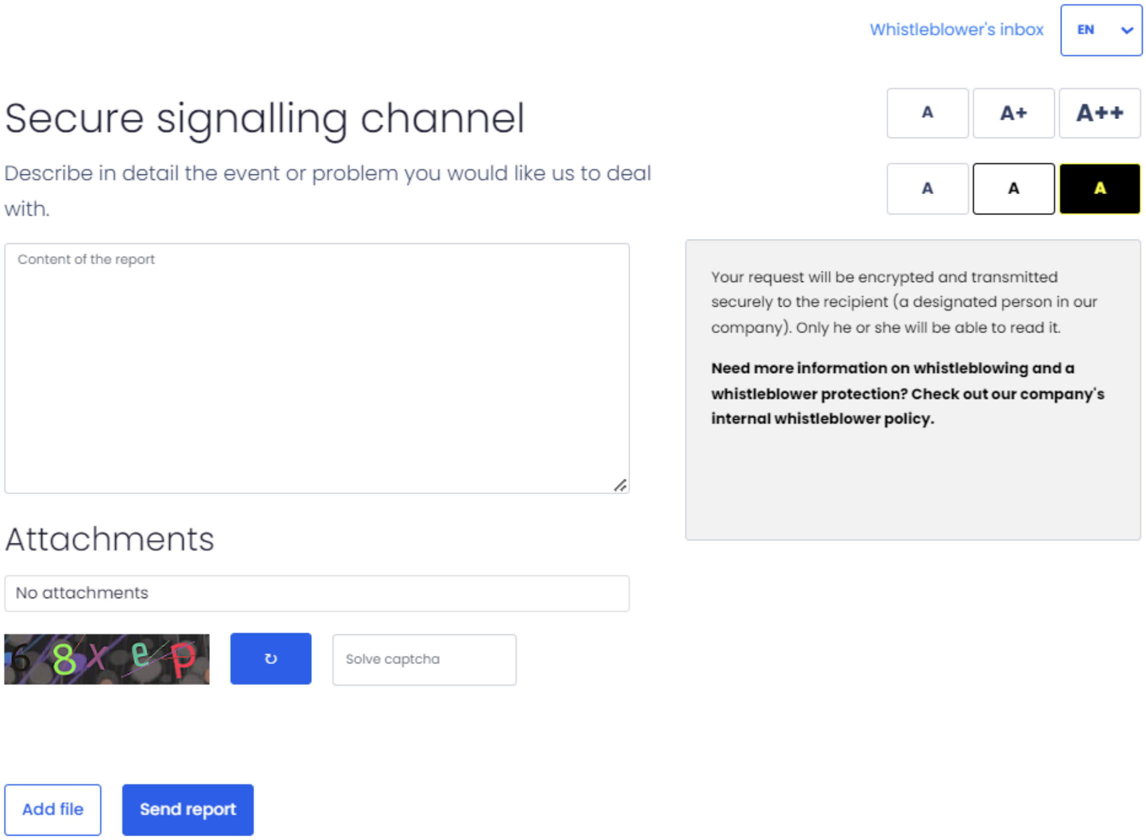
During the registration of each of the Recipients of Reports encryption keys (public and privated) are generated. They will be used to encrypt all the content stored on the server.

The whistleblower's form

In order to send a report to the company the whistleblower **should use the page with the company's chosen address** (sygnanet.pl/xxxxxx) on which the whistleblower's form can be found.

The whistleblower can choose from one of 12 available languages.

The form's content may be adjusted by the Principal Recipient of Reports (PRR) or the Administrator in terms of the wording and the checkboxes (for example the categories of the reports). These users decide also if a completely anonymous report is admissible.



Secure signalling channel

Describe in detail the event or problem you would like us to deal with.

Your request will be encrypted and transmitted securely to the recipient (a designated person in our company). Only he or she will be able to read it.

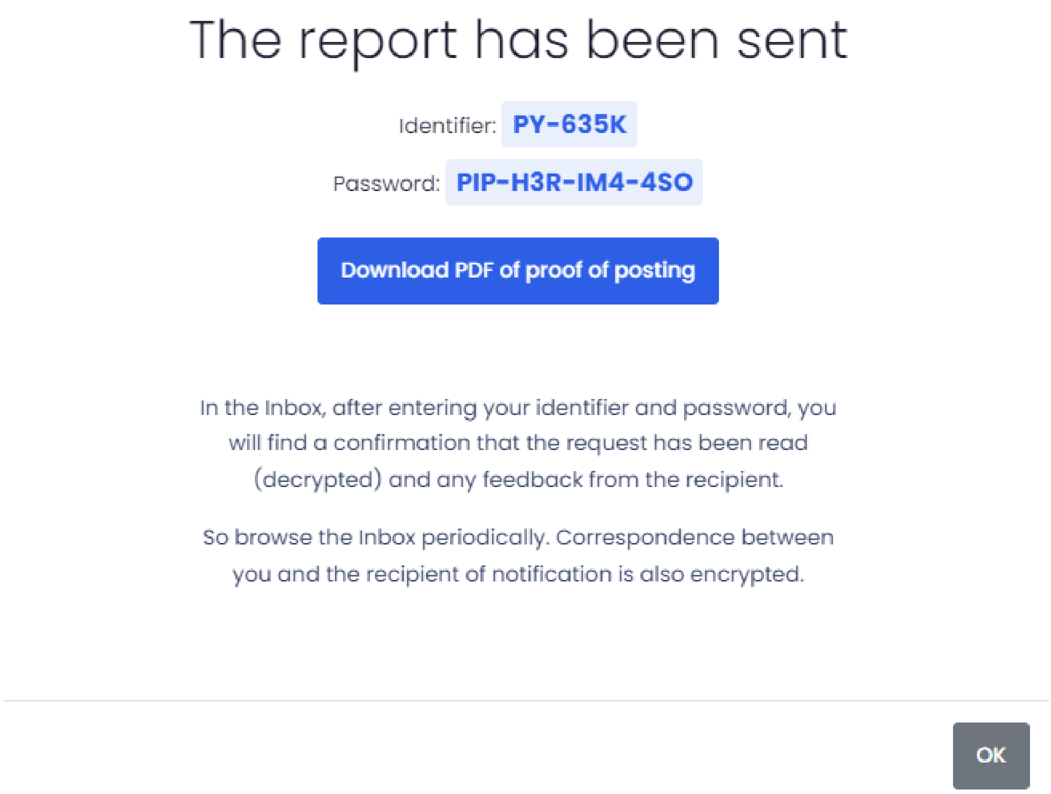
Need more information on whistleblowing and a whistleblower protection? Check out our company's internal whistleblower policy.

Attachments

No attachments

The whistleblower fills in the form with the content of their report and may also choose to attach files of any format. While the report is being sent to the service an identifier and a password are generated. They will serve any further (possibly anonymous) communication between the whistleblower and the employer. The whistleblower's form and the attachments are encrypted on the whistleblower's device using public encryption keys of the authorized Recipients of Reports and sent to the server. Encryption keys for that report are also generated. They will be used to encrypt the reply to the report.

After filing the report the whistleblower is shown **the identifier and the password associated with the report**. They can be saved as a PDF file.



The report has been sent

Identifier: PY-635K

Password: PIP-H3R-IM4-4SO

In the Inbox, after entering your identifier and password, you will find a confirmation that the request has been read (decrypted) and any feedback from the recipient.

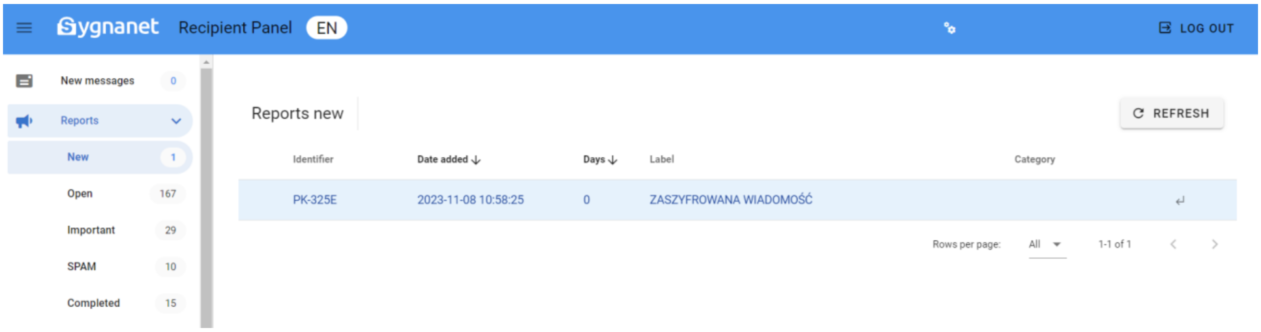
So browse the Inbox periodically. Correspondence between you and the recipient of notification is also encrypted.

On returning to the aforementioned page with the form, **the whistleblower may click on the link to the Inbox and log in using the assigned identifier and password to read the messages from the Recipent of the Report**. After that the whistleblower can continue to exchange messages with the Recipient of the Report in the same way.

Recipient Panel

A notification about a new report on the server is sent to the email address of the Recipient of Reports (authorized by PRR, for example to respond to reports from the given category). The Recipient then logs in to the system through that main page of sygnanet.pl by means of typing in the email address and the password, and is subsequently transferred to the Recipient Panel.

The Recipient Panel is available in 4 languages: English, French, German and Polish.

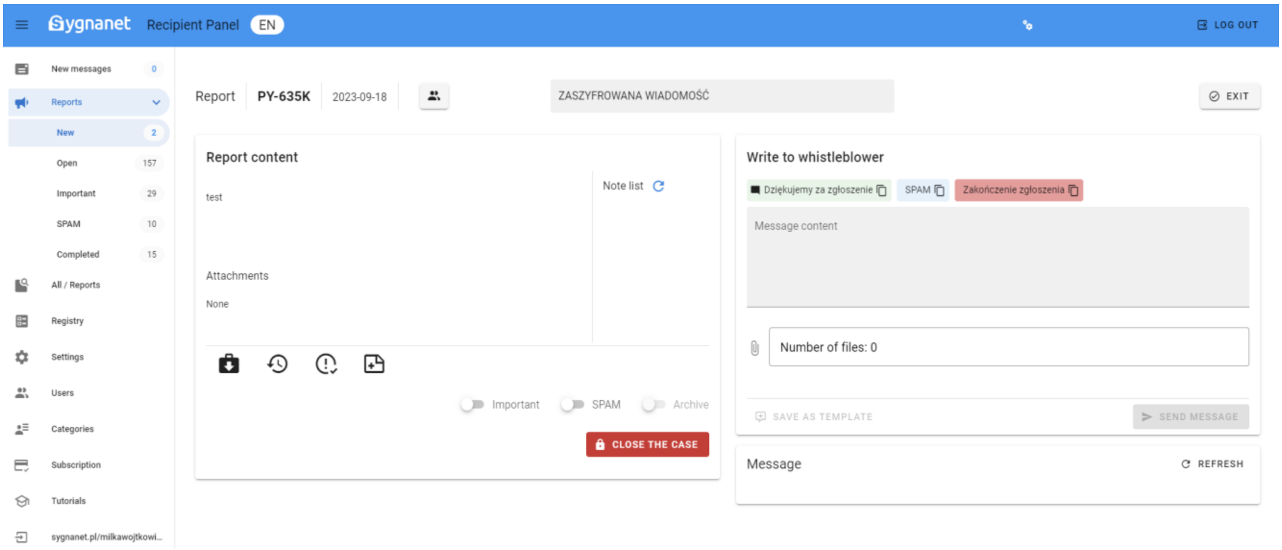


Reports new

Identifier	Date added ↓	Days ↓	Label	Category
PK-325E	2023-11-08 10:58:25	0	ZASZYFROWANA WIADOMOŚĆ	

Rows per page: All 1-1 of 1

On the left side of the Panel there is a menu leading to different functions of the service. **The new report is shown in the top tab called "Reports" and in particular the subtab called "New"**. The main box of the Panel contains then a list of new whistleblowers' reports. Each line of the list contains an Identifier, the date of filing and a "new report" label. By clicking on any of the lines of the report's description the Recipient is transferred to the page of the given report. **The report downloaded from the server is encrypted, so the first thing for the Recipient to do is to decrypt the report**. The Recipient does it using their password. The reported can now be further processed.



Report PY-635K 2023-09-18 ZASZYFROWANA WIADOMOŚĆ

Report content

test

Attachments

None

Note list

Write to whistleblower

Message content

Number of files: 0

Message

The subtab “New” leads only to those reports which haven’t yet been read by the Recipient. On the next log-in to the system the Recipient won’t see the description of the encrypted report in this subtab anymore. It will have transferred to the subtab called “Open”. It can be also seen in the tab called “All / Reports”.

Apart from “New” and “Open”, there are also subtabs called “Important”, “SPAM” and “Completed”. The Recipient can move the report to the latter three.

Messages to the whistleblower

After decrypting a new report the Recipient should **sent to the whistleblower a message confirming reception of the report** and any initial remarks concerning for example the need to supplement the report with further descriptions or documents. There are visible boxes in the Recipient Panel which serve to send messages to the whistleblower. They also contain previously prepared suggested messages. It’s also possible to set an automatic reply to the whistleblower to be sent automatically after the first decryption of the report. This can be done in the “Account management” tab (the two cogs next to the name of the logged in user).

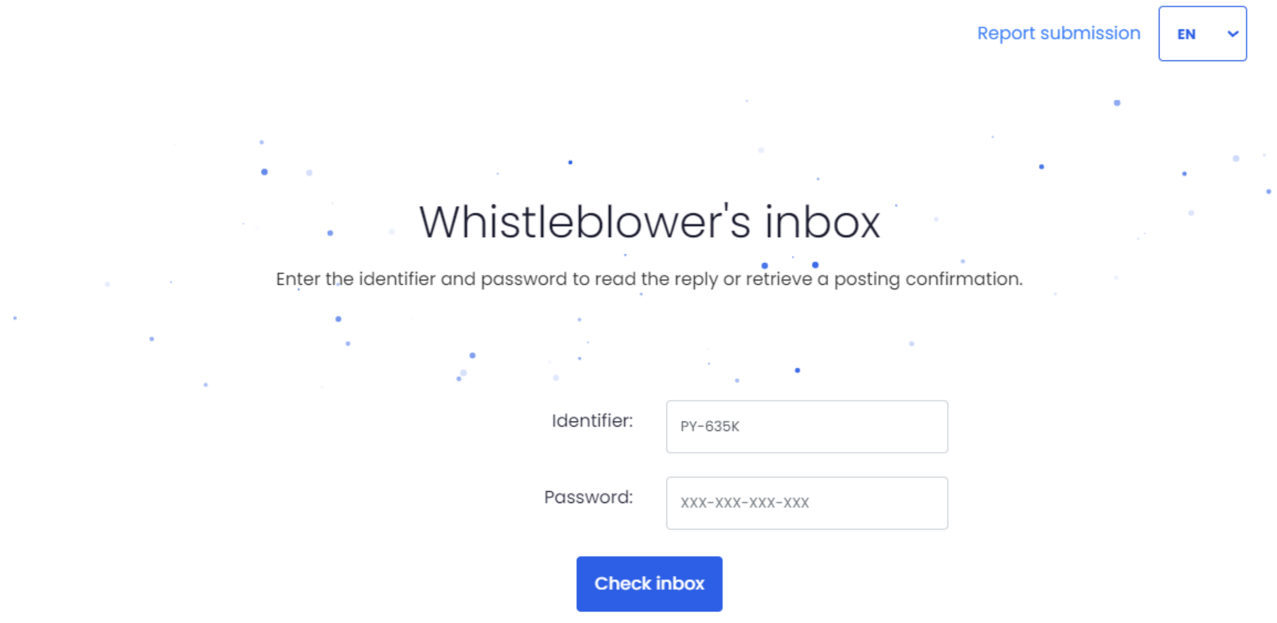
If the Recipient doesn’t send a message to the whistleblower in the first 7 days from the date of receiving the report, **the service will remind** them to do that via email.

The content of messages to and from the whistleblower can be found in the Recipient Panel below the box serving to send messages.

It’s good to know that the messages sent to the whistleblower are also encrypted with encryption keys created for the whistleblower when the report was filed. They’re then placed on the server in the encrypted form.

The whistleblower wishing to follow up on their report will check its status logging in from time to time on the familiar page used earlier by them to file the report (sygnanet.pl/xxxxxx).

The whistleblower will then click on the “Inbox” link and will be asked to provide the log-in details sent to them upon filing of the report:



Report submission EN

Whistleblower's inbox

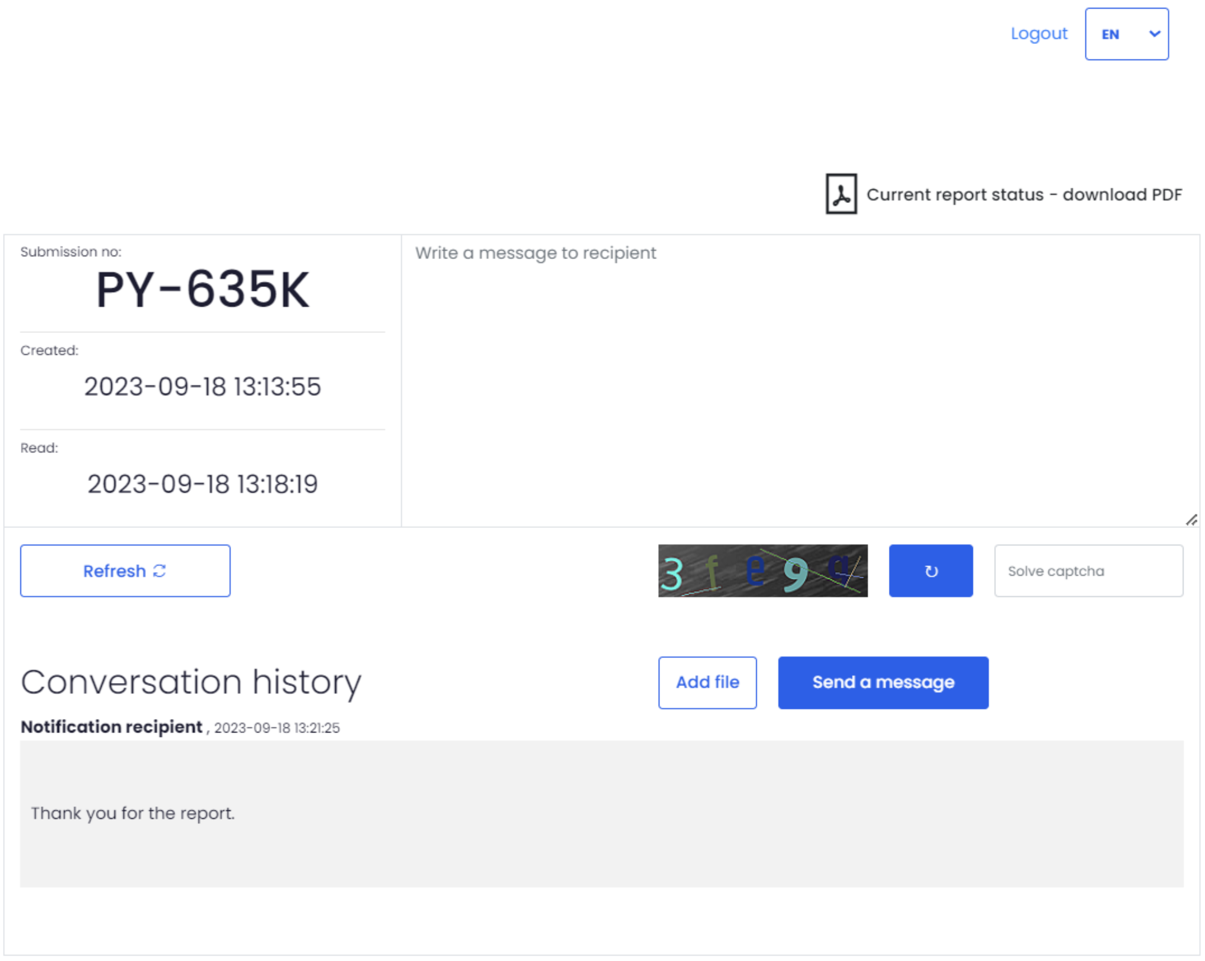
Enter the identifier and password to read the reply or retrieve a posting confirmation.

Identifier: PY-635K

Password: XXX-XXX-XXX-XXX

Check inbox

If the log-in details are correct, the whistleblower will decrypt and read the current status of the report and the reply from the Recipient, and **may continue to exchange messages** with the Recipient.



Logout EN

Current report status - download PDF

Submission no:
PY-635K

Created:
2023-09-18 13:13:55

Read:
2023-09-18 13:18:19

Write a message to recipient

Refresh

Solve captcha

Conversation history

Add file

Send a message

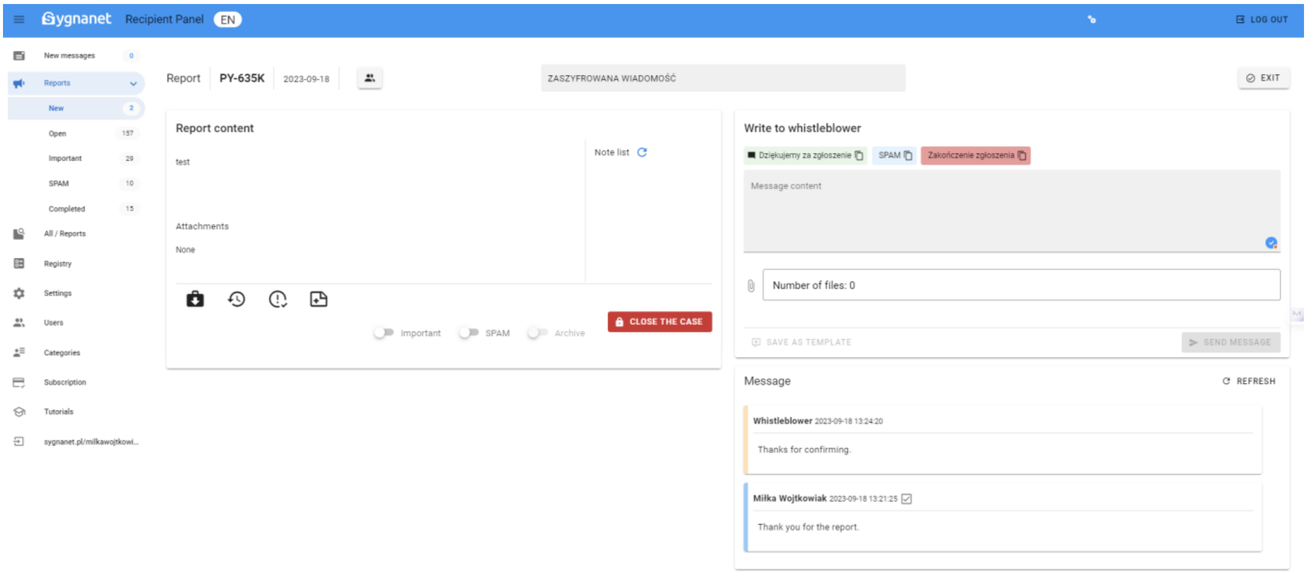
Notification recipient , 2023-09-18 13:21:25

Thank you for the report.

Sygnanet

When the whistleblowers sends new messages concerning the previously sent report, a notification is also sent to the Recipient's email address. In this way, the Recipient is notified each time about a need for a reaction on their part.

After logging in to the service the Recipient may click on the "New message" tab in the Menu and decrypt the content of the report and messages from the whistleblower.



ZASZYFROWANA WIADOMOŚĆ

test

Attachments: None

Number of files: 0

Whistleblower 2023-09-18 13:24:20

Thanks for confirming.

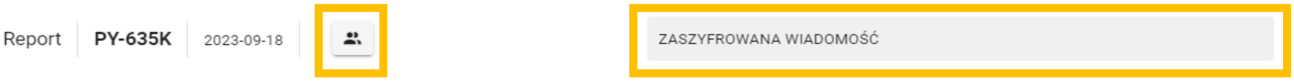
Miłka Wojtkowiak 2023-09-18 13:21:25 ☑

Thank you for the report.

Processing the report

On the screen showing the content of the report and the messages to and from the whistleblower, there also **various icons and buttons** allowing several ways to process the report.

In the top line above the box with the content of the report:

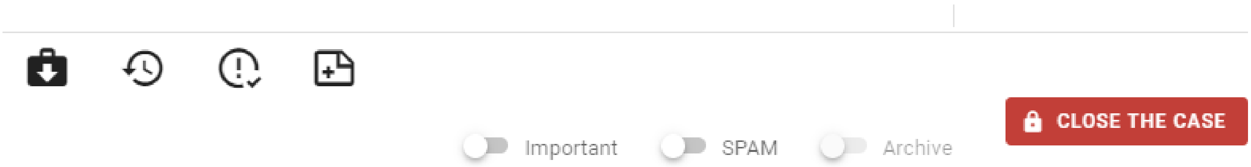


ZASZYFROWANA WIADOMOŚĆ

The icon 👥 can be used to show a list of people with access to the report. It also allows to block and grant access to a different person.

The box saying "ENCRYPTED MESSAGE" (zaszyfrowana wiadomość) is an initial label of the report. It is advisable to change this label to something specific related to the content of the report, for example "Bus for the employees".

The icons in the content box allow the following actions:



allows to compress all the documents (in .pdf) related to the report to one .zip file and download them to the Recipient's device (in non-ecrypted form!)

allows to see the history of all the actions performed in relation to the report

allows to create or to edit the Final Protocol (containing a form with some pre-made parts, including those which are required by the law)

allows to add notes to the Report: private (visible only for the person who added them) or public (visible to anyone who has access to the report)

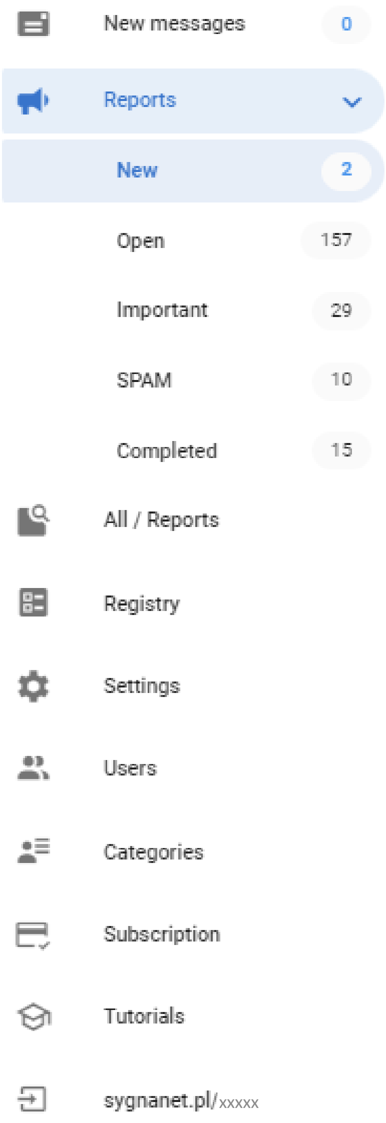
Buttons ○ Important ○ SPAM ○ Archive may be used to move the report to the given category (only completed reports may be sent to the Archive - they won't be seen anymore on the list of reports).

The button CLOSE THE CASE should be used to finalize the processing of the report. This status will be then shown everywhere next to this report and the report itself will be moved to the Reports / Completed category.

Each **report should be processed for no longer than 3 months** and the whistleblower has a right to be informed about the way in which it is processed and the actions taken. The service sends a notification to the Recipients 14, 7 and 1 day before this date. If there are reasons for exceeding this deadline, the whistleblower should be made aware of this.

Recipient Panel Menu

The above has been a description of processing of the report in the tab Reports of the main Recipient Panel Menu (on the left side of the Recipient Panel). The following is a description of the rest of the tabs:



New messages - here new messages from the whistleblower can be found, pertaining to reports which are already being processed.

Reports - the tab described above, with several subtabs.

All / Reports - contains a list of all reports which can be filtered in various ways.

Registry - contains all the legally required elements of the reports registry and is created automatically. A more detailed description of the registry can be found in our tutorials.

Settings - allows the company to edit the whistleblower's form, add company logo to the form, edit the footer of PDF documents, set two-factor authentication. A more detailed description of settings can be found in our tutorials.

Users - allows adding users (recipients) and modifying their access. A more detailed description of users can be found in our tutorials.

Categories - here one can create categories of reports, make them visible in the whistleblower's form (so that the whistleblower can choose the category themself) and assign recipients to service the given category. A more detailed description of categories can be found in our tutorials.

Subscription - contains information about the maximum number of users (recipients) allowed within the active plan as well as the date when the plan ends and the cost of prolonging the subscription. The service sends out a notification about the approaching end date. After that date the access to the reports is blocked. Prolongation of the subscription is possible in this tab (even after the access to the reports is blocked).

Tutorials - link to many different training materials, videos and documents about the service, whistleblowers' rights and technical details of the service (https://zapis.specfile.pl/wdrozenie_systemu).

Sygnanet.pl/xxxxx - link to the whistleblower's form. It's also useful when designing the form. It can be used to manually create reports received for example on the phone or in writing - in order to keep all the reports in one safe (encrypted) place and have a complete register of all the reports.

Tutorials

Our tutorials (https://zapis.specfile.pl/wdrozenie_systemu) contain further detailed instructions and descriptions of the specific operations which can done using the service. Tutorials are both videos and PDFs. They include:

□ Registration in Sygnanet.pl

□ Presentation of reception and proceeding of the report in the Recipient Panel of Sygnanet.pl

□ Presentation of “All / Reports” tab in the Recipient Panel of Sygnanet.pl

□ Presentation of “Registry” tab in the Recipient Panel of Sygnanet.pl

□ Presentation of “Settings” tab in the Recipient Panel of Sygnanet.pl

□ Whistleblower’s form

□ Presentation of “Users” tab in the Recipient Panel of Sygnanet.pl

□ Presentation of “Categories” tab in the Recipient Panel of Sygnanet.pl

□ Automatic confirmation of the reception of the report

□ Manual adding of the report to the Recipient Panel

What is more, tutorials include recordings of webinars where our specialists present functions of the service and answer audience’s questions. There are also materials which the company can use to train employees to use our service.

Apart from tutorials our clients also get an online training for their employees and internal procedure benchmark prepared a lawyer - a specialist in the field.

A lot of important technical details can be found in the Sygnanet service specification annexed below.

SYGNANET Specification

Service’s web address:

www.sygnanet.pl

Purpose:

An online platform for receiving and processing whistleblowers’ reports. Anyone connected to the given company can be a whistleblower: an employee, a client, a contracting party. Reports may concern infringements or remarks related to the company’s activity or employment issues. The company appoints a person (for example a compliance officer or an HR representative) to be a recipient of whistleblowers’ reports.

Requirements:

The only requirement for filing and processing reports is the use of any internet browser on a desktop or mobile device.

Web address for whistleblowers in the given company:

On the Sygnanet server there is a dedicated web page for any company using the service where whistleblowers may file a report. The address of the page is:

sygnanet.pl/name

where name - name set by the given company.

Servicing whistleblowers:

The recipient of reports makes a decision about the way in which reports are to be filed. There are there options to choose from:

a) a form requiring whistleblower's personal data - to file a report the whistleblower has to fill in the boxes required by the recipient of reports;

b) a form allowing to enter the whistleblower's personal data - the whistleblower decides whether to fill in additional boxes provided by the recipient of reports;

c) an anonymous form - the form contains only a box for the content of the report and attachments (if there are any). No data about whistleblowers is gathered. There's no possibility to track the whistleblower's personal data, location information or IP address.

Technology assuring whistleblowers' anonymity:

Anonymous proxy server which doesn't log data transmission and connects transmissions to various servers, including to the sygnanet.pl server, which also doesn't log transmission. In this way, no historical data about connecting to the sygnanet.pl server is created. Both servers are placed on a platform belonging to Sygnanet owners (Specfile Project Sp. z o.o.). For the sake of anonymity the sygnanet.pl server is not shared to the recipient's (companies using Sygnanet) infrastructure.

Filing a report:

To file a report one must place its content in the text editor box on the assigned website. There's also an option of uploading attachments. The whistleblower might be asked to fill in additional boxes and to choose a category of the report from the list of categories provided by the company.

Protecting the content of whistleblowers’ reports:

Encryption of the content of the report takes place on the whistleblower’s device (browser) in a way which makes it possible only for the assigned recipient to read the report. The report is sent to the server in the encrypted form. There’s no way to read it on the server. The server doesn’t take part in the encrypting or decrypting of reports. These operations are done only on the whistleblower’s and the recipient’s devices.

The way encryption works:

The assigned recipient of reports generates their first pair of keys (private and public) while registering in the service for the first time. The public key of the recipient, downloaded from the server to the whistleblower’s browser, is used to encrypt the whistleblower’s report.

Encryption method:

The process of encryption and decryption of the report file is based on RSA-4096 (of keys private and public) and AES-256 algorithms, which are used around the world to keep information secret. They’re considered a standard in cryptography because of their security.

Getting the reply:

As the report is being filed, encryption keys, the report identifier and the inbox password are generated for the whistleblower. The whistleblower may use them later to read the reply from the recipient of the report. If the whistleblower filed the report anonymously, all contant between the whistleblower and the recipient of the report remains anonymous.

Whistleblower’s documents:

After filing the report, the whistleblower receives a PDF file with a confirmation that the report has been filed. It can be downloaded or printed out. The file contains the date and the content of the report, a list of the attachments, the identifier and the password (to be used in case of further contact) and the address of the page on the server which can be used to contact the recipient again. A similar confirmation, containing messages to and from the recipient of the report, may be downloaded from the whistleblower's inbox after each contact with the recipient of the report.

Notification about a new report:

When the server gets an encrypted file with the report from the whistleblower, the recipient (the person assigned by the company to process the reports) is sent an email notifying them about a new report and a link to the page in the Sygnanet service which can used to process the report.

The way and place of decrypting the report by the recipient:

The recipient logs in to the service and gets access to the recipient panel which contains a list of reports. Using the browser the recipient downloads the encrypted report from the server and decrypts it on their own device. No decrypting is made on the Sygnanet server.

Functions available to the recipient of the report:

- ❑ Choice of the language version of the whistleblower's form (12 languages)
- ❑ Choice of the language version of the recipient panel (4 languages - English, French, German, Polish)
- ❑ Adding/removing recipients and their access
- ❑ Labelling the report
- ❑ Moving the report to Important, SPAM, Archive, Completed
- ❑ Creating notes
- ❑ Creating the final protocol

- ❑ Creating and browsing the messages to the whistleblower (including attachments exchanged in the entire processing of the report)
- ❑ Creating model replies
- ❑ History of operations (the report, all the users)
- ❑ Saving the decrypted report and messages for archival purposes (downloading the files from the system)
- ❑ Notifying the recipient about deadlines for processing reports
- ❑ Reporting to senior staff
- ❑ Automatic Register of Reports
- ❑ Two-factor authentication as an option
- ❑ Freely creating the whistleblower's form
- ❑ Categorizing reports

The number of possibilities to edit the whistleblower's form and the list of functionalities are continuously growing.

Recipient's reply to the whistleblower:

The recipient of reports can create a reply to the whistleblower and place it on the server. The server will then assign it the right identifier and password (generated previously for the whistleblower). When the whistleblower connects with the server again and enters the identifier and the password they will receive the message from the recipient. The whistleblower may then reply to the message or save it (print it out). The anonymity of contact and the encryption of content remain in place.

Registration of a company in the service:

A company can be registered online through a form found on the main site of the sygnanet.pl service. Registration requires entering an email address of the principal recipient of reports assigned by the company and setting a name for the company in the service (which will become part of the web address for whistleblowers). Company's data is then verified on the basis of the subscription fee bank transfer.

Recipients of reports' roles in the company:

The first email address entered at the registration of the company determines who is the Principal Recipient of Reports. The PRR then may add other recipients to the service and grant them different levels of access: Principal Recipient, Recipient, Administrator, Auditor.

Information about the service's allocation and the processing security:

Sygnanet is a part of Specfile Project Sp. z o.o.'s platform used as a cluster on two computer sets located in OVH centres in Warsaw (Poland) and Roubaix (France). OVH stores the service hourly. OVH guarantees the 99,5% availability of the service. Specfile Project Sp. z o.o. assumes 97% availability in its contracts with clients. Online storage of services and databases is also done once a day on our company's server, maintained by Horyzont in their datacentre in Poznań (Poland). Organizational and technical principles upheld by Specfile Project Sp. z o.o. are specified in the documents: Cyber Security Policy and Personal Data Protection Politics.

Information about the creators of Sygnanet service:

Specfile Project Sp. z o.o.
ul. Nagórskiego 3, 60-408 Poznań,
Tel. +48 501 34 12 77

The creators of the service are also known for lauching such services as Przelewy24.pl, specprawnik.pl, specfile.pl, bilety24.pl, 3gry.pl

The year of production:

2021