GUIDE TO USING THE GLOBALEAKS PLATFORM

Administrators

Whistleblowing Solutions[1] (WBS) is a non-profit social enterprise that supports the fight against corruption through the research, development and provision of specific digital technology and operational support to anti-corruption organisations. These organisations, in turn, support whistleblowers in reporting malpractice worldwide.
The goal of WBS is to support the development of the GlobaLeaks free software and to foster a large community of those who support whistleblowers.

This guide was produced with financial support from the European Union under the "Strengthening Accountability Networks among Civil Society" and the "Speak Up Europe" projects. The content of this guide represents the views of the author only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Funded by
the European Union

Guide to using the GlobaLeaks platform. Administrators

Author: Maria Sideri (Transparency International Secretariat)

Contributors: Giovanni Pellerano, Susanna Ferro (Whistleblowing Solutions) Anoukh de Soysa, Marie Terracol, Aram Khaghaghordyan, Shubham Kaushik (Transparency International Secretariat), Donncha Ó Giobúin (Transparency International Ireland), Vasja Cepic (Transparency International Slovenia), Giorgio Fraschini (Transparency International Italy)

[1] Social Enterprise - Whistleblowing Solutions (https://www.whistleblowingsolutions.it/)

WHAT IS THE PURPOSE OF THIS GUIDE?

This guidance has been developed to accompany the roll-out of the GlobaLeaks platform to interested organisations. It is a step-by-step guide created to explain how to customize the GlobaLeaks platform by setting up basic configurations.

As the administrator of the platform, you will not have access to the whistleblowers' reports. Your role will be to perform platform configurations, support the organisation's staff receiving the whistleblowers' reports in their operation, as well as to establish best practices and ensure that every user implements them.

CONTENTS

GLOSSARY

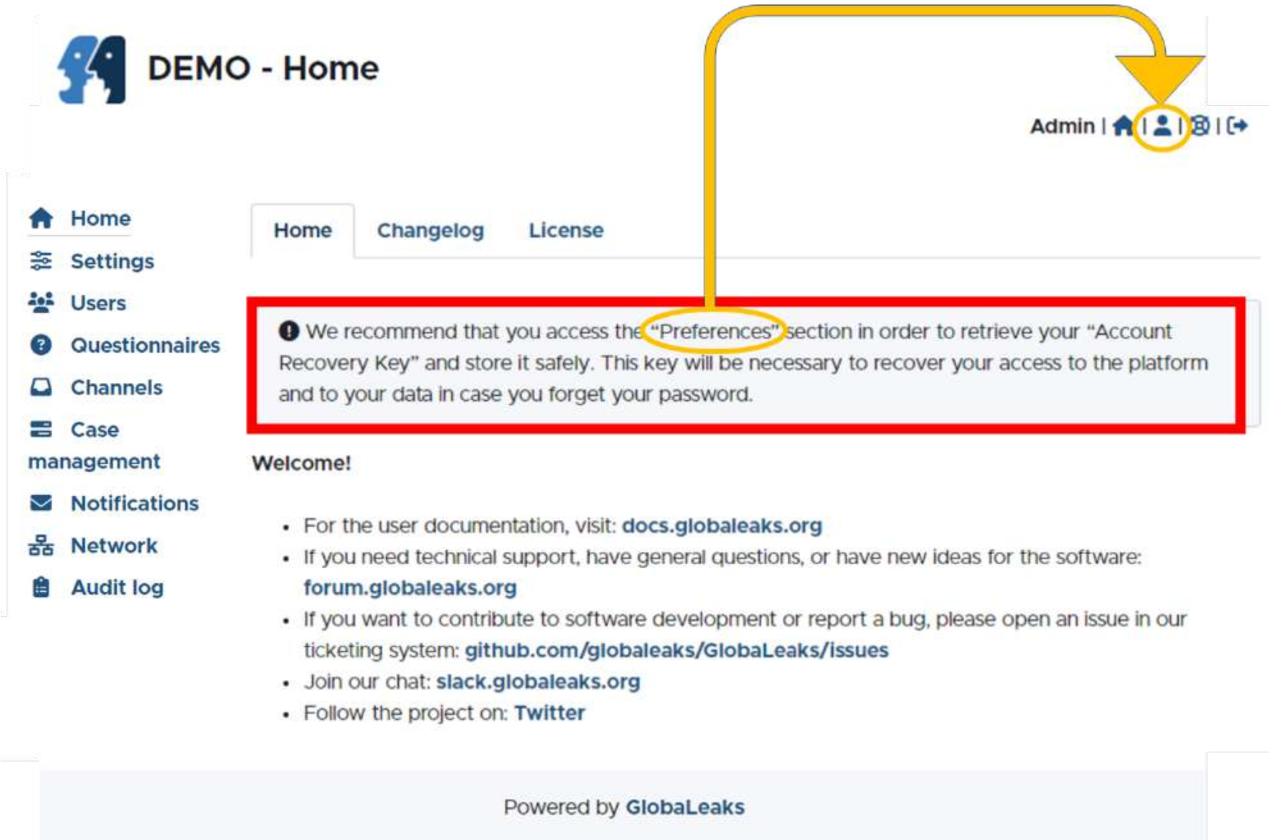
- **Administrator**
  The user who is running the GlobaLeaks platform. Administrators perform the maintenance and overall management of the platform and provide technical assistance to the organisation staff managing the whistleblowers reports. Administrators do not have access to whistleblowers' reports.
- **Whistleblower / Reporting person**
  The user who submits a report through the GlobaLeaks platform.
- **Channel**
  The platform's reporting channel; it can also be an area of issues addressed by the organisation (e.g., Corruption-related complaint). The platform offers the possibility for more than one reporting Channels (Contexts), offering the whistleblowers the option to select the topic of their report and submit through the appropriate reporting channel. Also, each reporting channel could be assigned to and managed by a different recipient.
- **Notification**
  The email sent to inform a recipient of a new report, or an update relating to an existing report.
- **Platform**
  The system running the GlobaLeaks software.
- **Questionnaire**
  The set of questions that a whistleblower is asked to answer in order to file a report.
- **Receipt**
  The random 16-digit code generated by the system and provided to whistleblowers upon the submission of their report, enabling them to access and update their report by adding comments and new files/evidence.
- **Recipient**
  The user enabled to read, verify, and analyse whistleblowers' reports. Recipients may also communicate with whistleblowers via the platform to solicit additional information and evidence, by exchanging messages.
- **Report**
  The object of a whistleblower's submission, including answers to a questionnaire and attached material.
- **Submission**
  The action performed by the whistleblower when filing a report.

I. GETTING STARTED

FIRST LOGIN

Once the new user account is created, you will receive an "Account Activation" email, containing your Username and an activation link.

By clicking on the activation link the system will invite you to create your password, and then direct you to your homepage. There, you can find useful links for GlobaLeaks user guidance, software security, best practices, and community support[2] – and an **important recommendation**:



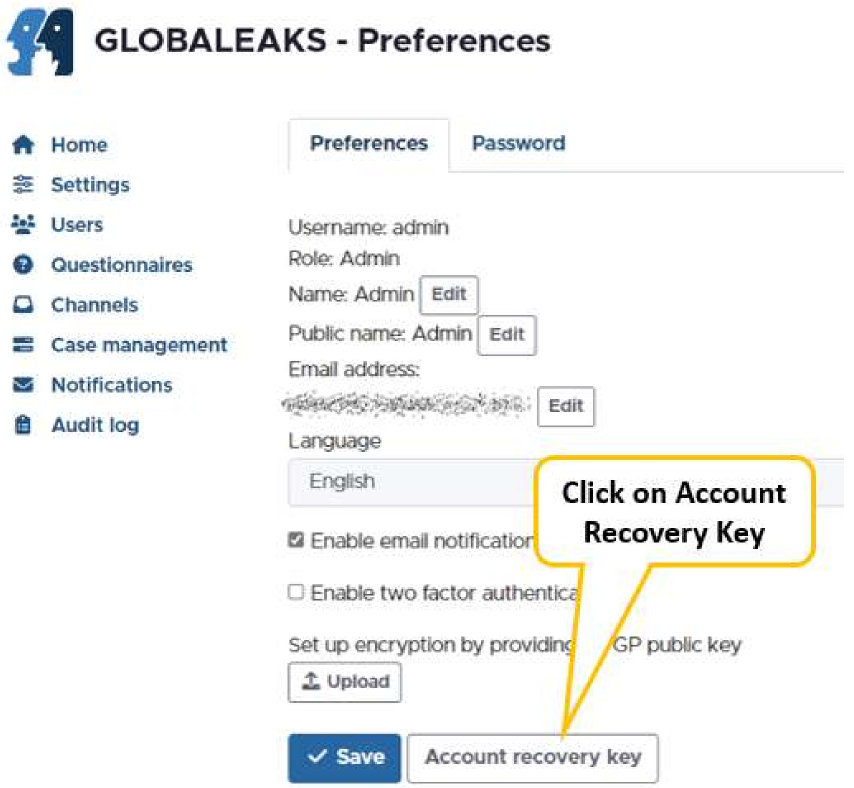
[2] if you encounter a problem using the platform, create an issue on the GlobaLeaks ticketing system [https://github.com/globaleaks/GlobaLeaks/issues] and help improve transparency worldwide!

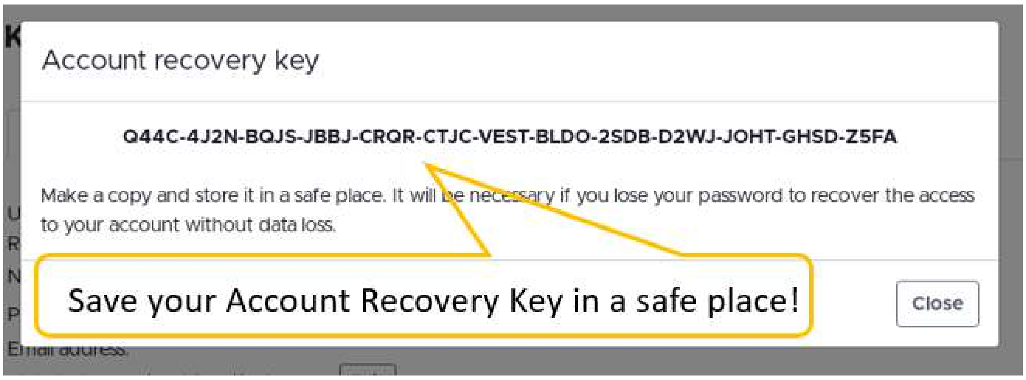
ACCESS AND SAVE YOUR ACCOUNT RECOVERY KEY

After first login, you should access your **Account Recovery Key** on the **Preferences** page.

IMPORTANT NOTE

This is a *fundamental step* that all Users should do at their first login after activating their account to back-up their own account recovery key. This is **of particular importance to Administrators**, as they can restore account access to Recipients who have lost both their password and account recovery key, and therefore **prevent data loss**

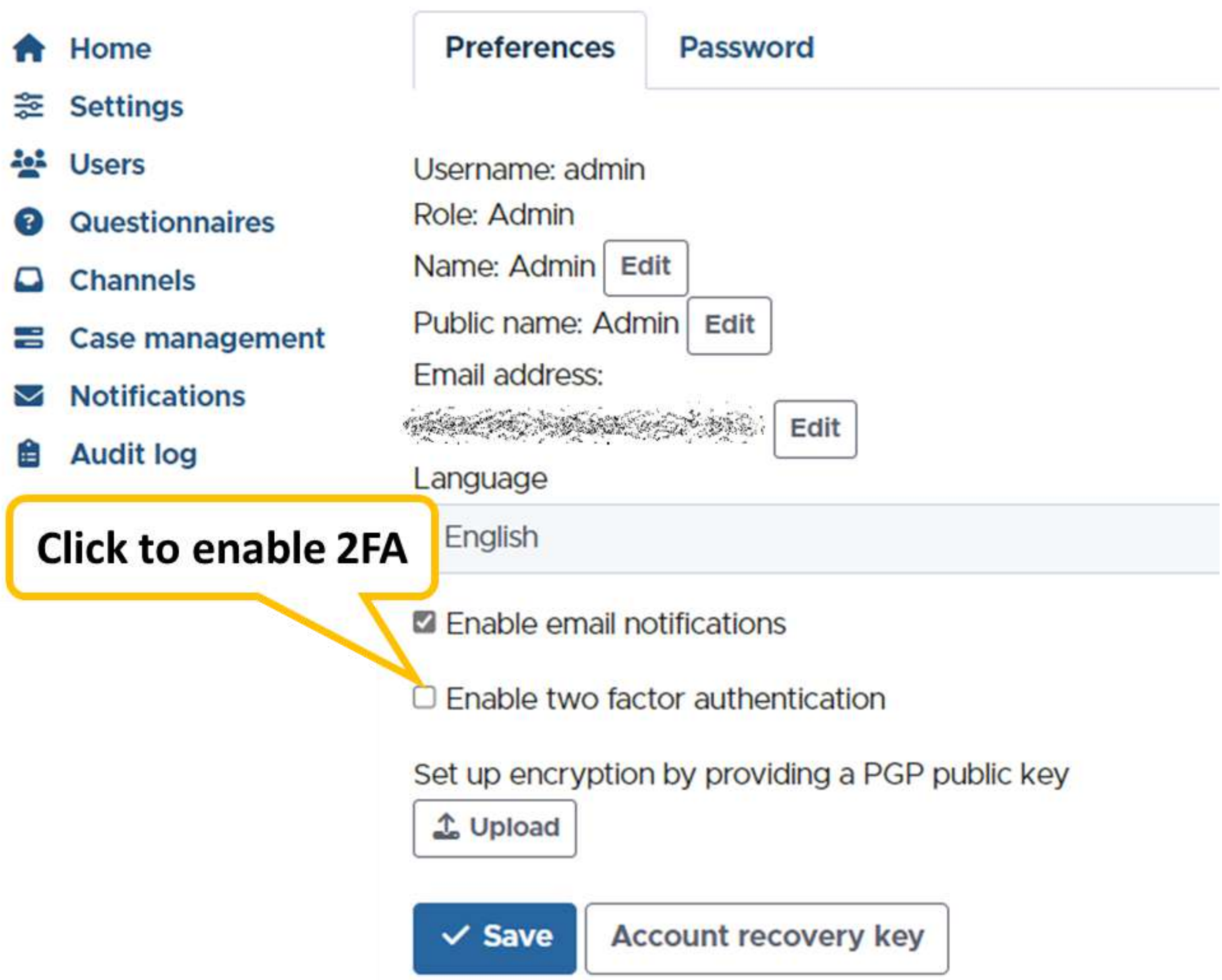




Please consider storing your Account Recovery Key in a very *safe* place; in case you write it down by hand, ensure that you *clearly* mark the numbers and letters so that it will not be difficult to read when you need to use it (for example, discerning the difference between a zero (0) and the capital letter O is a common difficulty).

ENABLE TWO-FACTOR-AUTHENTICATION (2FA)

After accessing your Account Recovery Key, you have to enable and configure **two factor authentication** (2FA) for extra security.



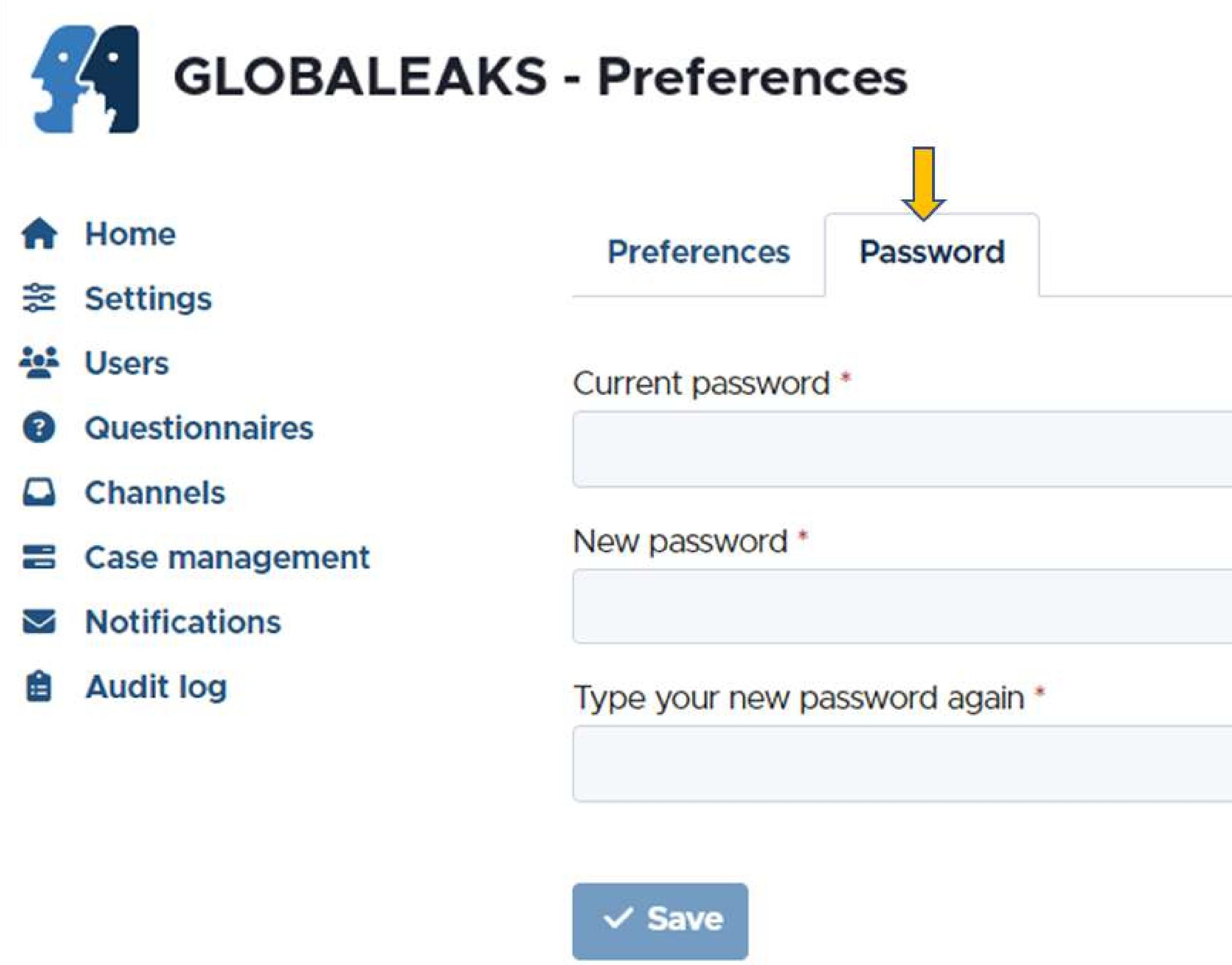
For this, you will also need to install an Authenticator App on your phone.[3] Use the app to scan the code shown to set up a time-based code

[3] You can download a commercial app like the Microsoft or the Google Authenticator Apps for Android phones on Google Play and for iOS phones on the App Store. Alternatively, you can download an opensource app like https://freeotp.github.io/.

CHANGE YOUR PASSWORD

You can change your password at any time by accessing the **Password** tab present in the **Preferences** page.

Please note that the system prompts users to change their password periodically for security purposes.[4]

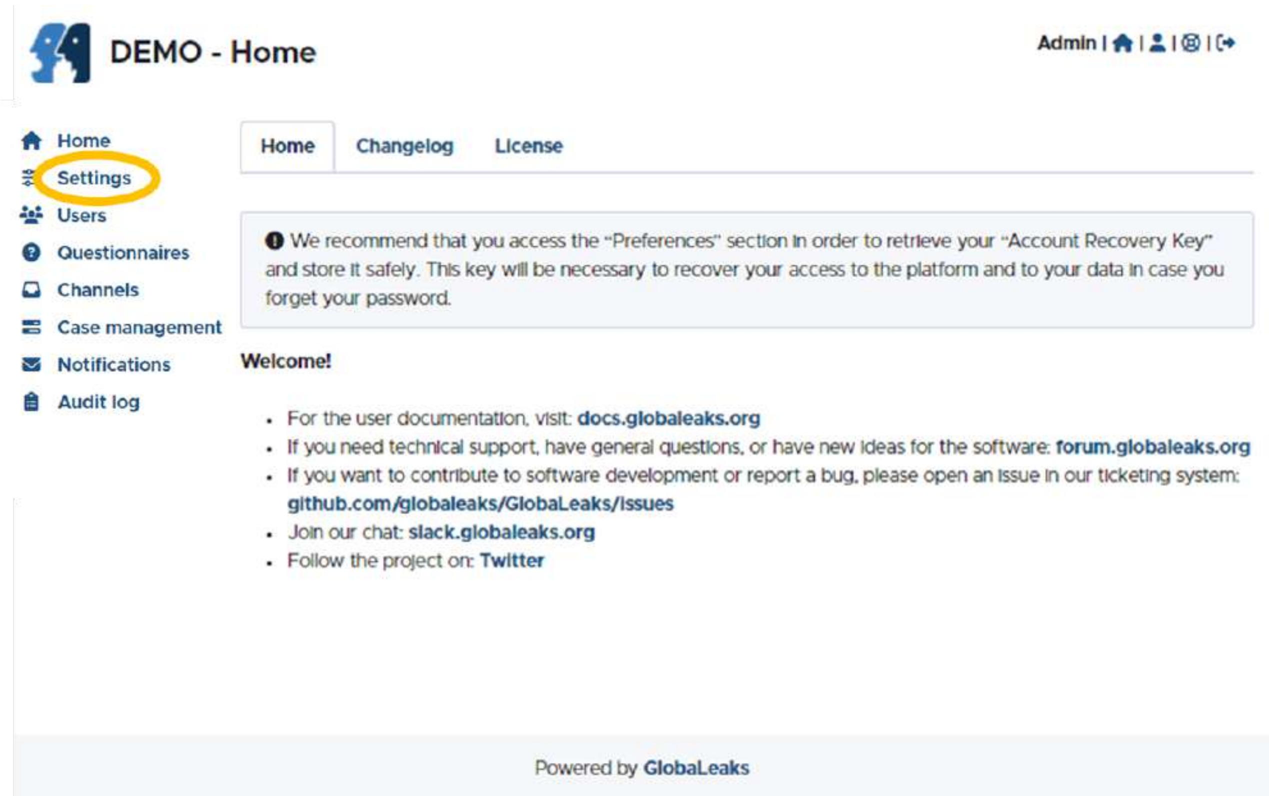


[4] Consider using an app like the KeePassXC [https://keepassxc.org/] to securely manage and store your passwords.

II. COMMON CONFIGURATIONS

CUSTOMISE THE INTERFACE

From your Homepage, choose **Settings** from the menu on the left.



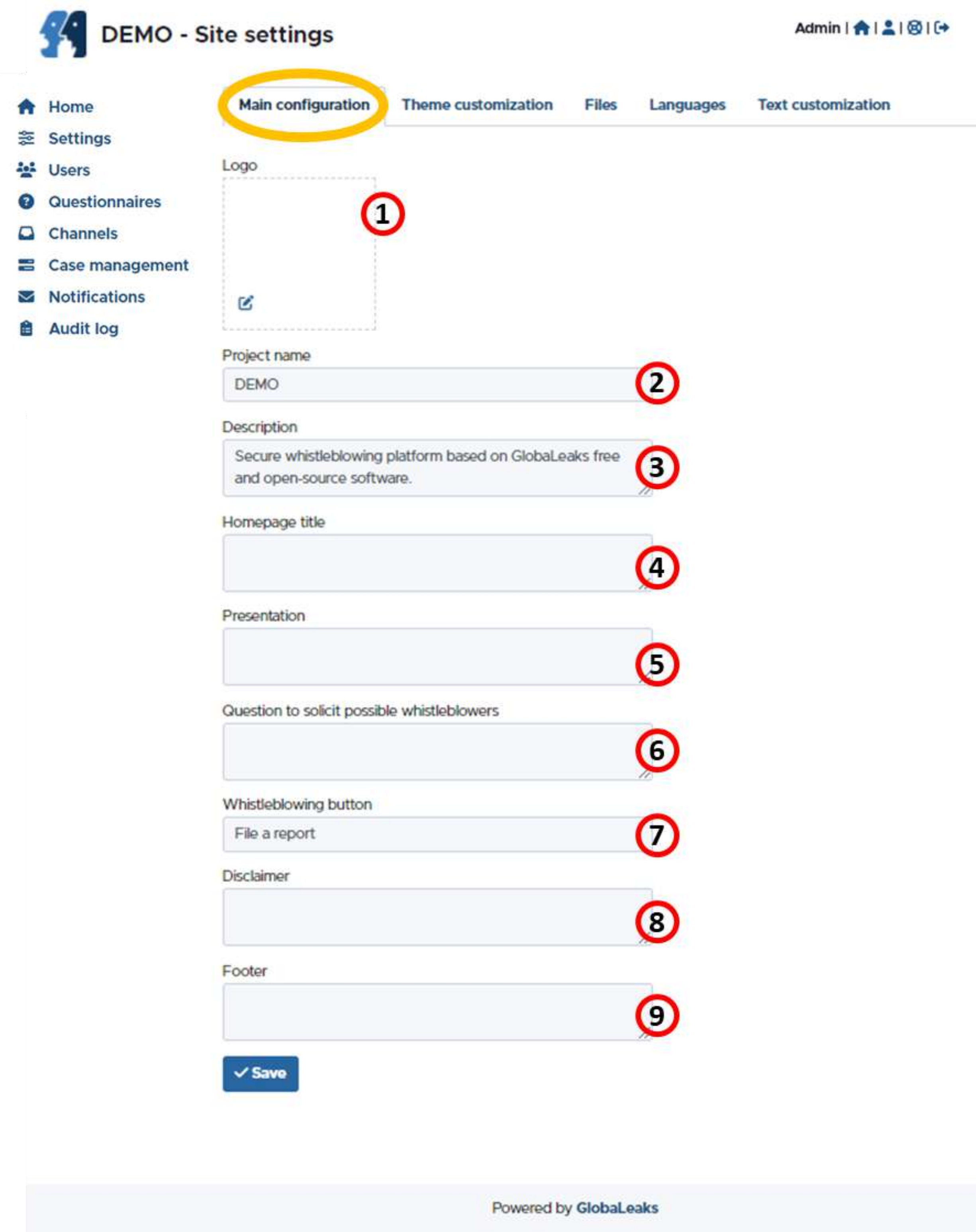
MAIN CONFIGURATIONS

You can customize your platform interface:
(also see images and example below)

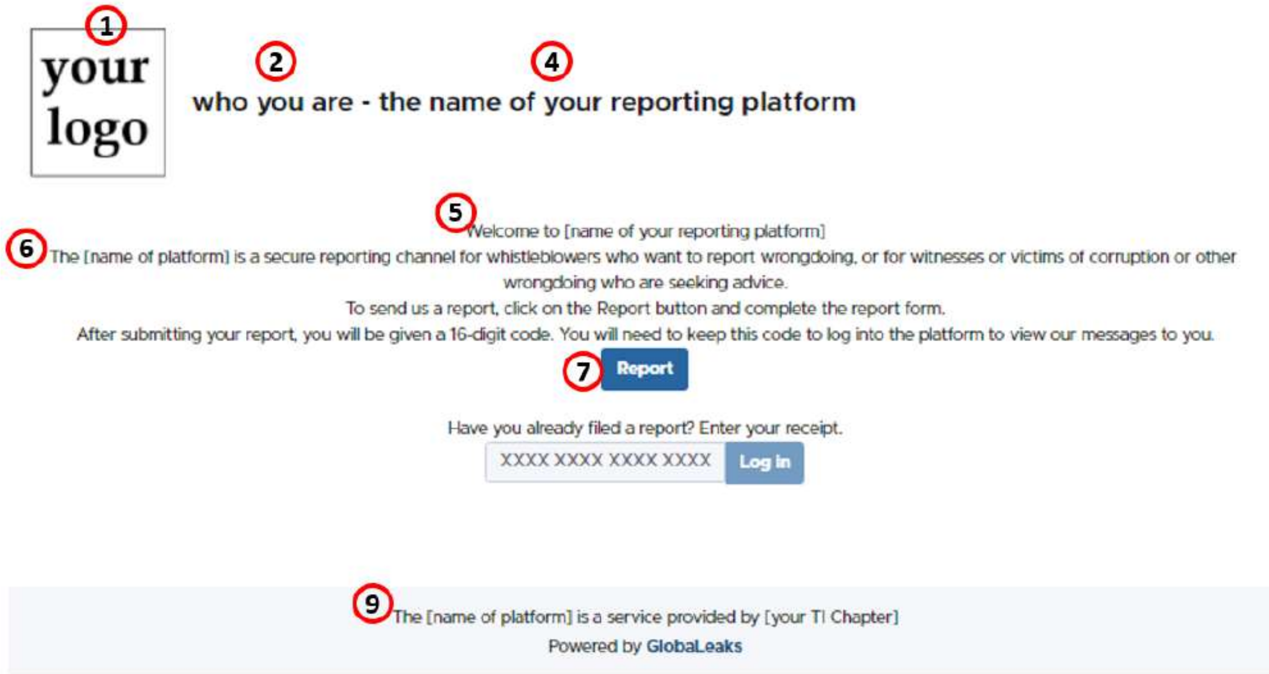
Change the *Logo*
Change the *Project name*
Add a *Description* for the search engine results

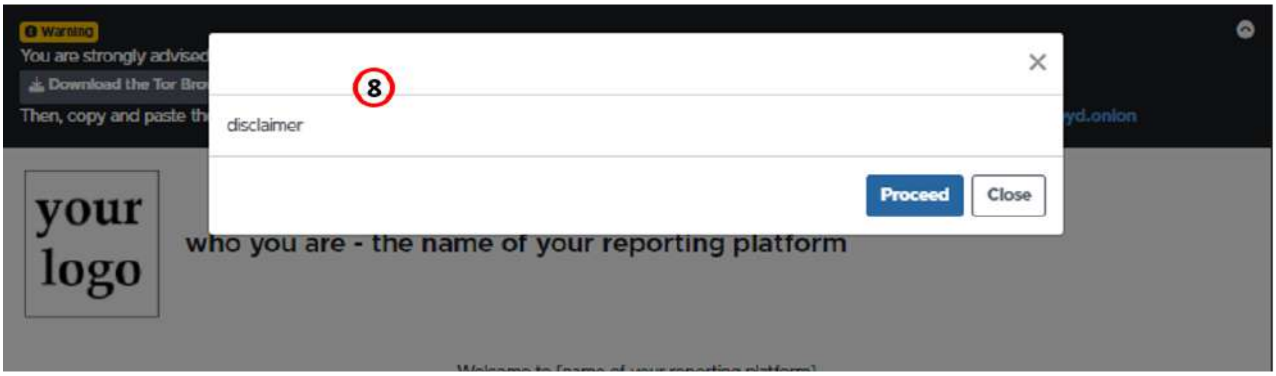
e.g.

Add a *Homepage title*
Add a *Presentation*
Add a message to potential reporting persons/whistleblowers
Customize the *Whistleblowing button* (i.e. the button which navigates to the Report page)
Add a *Disclaimer*, it will pop up before navigating to the Report page
Add a *Footer*



This is an **example** of what the customized interface could look like:





***tips**:

— to insert a hyperlink (e.g. to your organisation), wrap the link text in brackets `[text link]` followed by the link wrapped in `(link)` parentheses

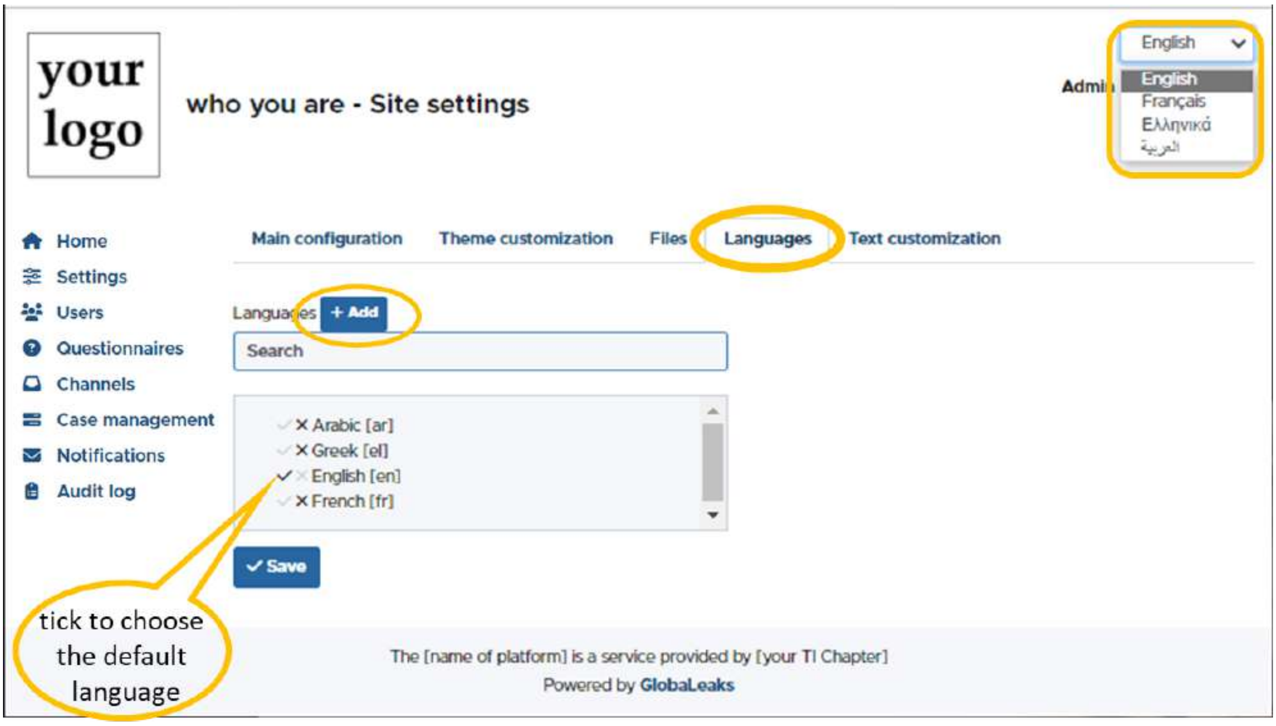
— to make text *italic*, wrap it in asterisks `*text*`

— to make text **bold**, wrap it in double asterisks `**text**`

— to create a heading, add one or more hash signs (#) before the heading text; the number of # used will determine the heading size, ranging from one `#the largest heading` to six `######the smallest heading`

LANGUAGES

You can localize your platform by adding/removing languages; you can also set the default language.[5]



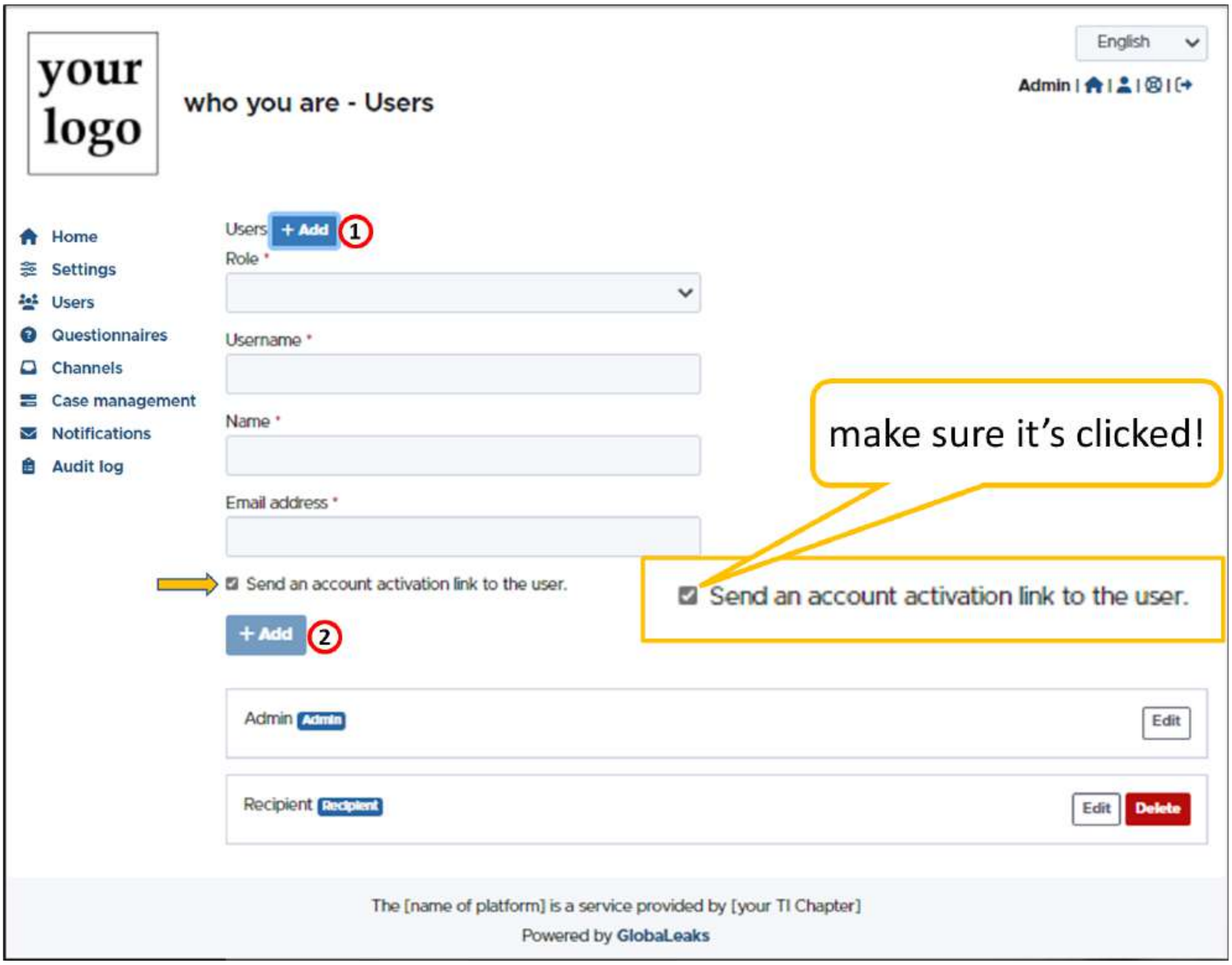
[5] The GlobaLeaks software is already available in more than 90 languages and is continuously being translated to more, thanks to the Localization Lab [https://www.localizationlab.org/] and a great volunteer community. In case you find that a language required for your project is not available, we invite you to register on the web translation platform [GlobaLeaks localization (transifex.com)] offered by Transifex [https://www.transifex.com/] and support the translation process.

CONFIGURE THE USERS

After the basic configuration is completed, the platform is configured with two users, an Administrator and a Recipient. You can add (or remove) users, assign user roles (Administrator / Recipient), and manage their respective privileges. You can have one or multiple Recipients per Channel, and/or have one Recipient accessing multiple Channels.

Please note that, as the Administrator of the platform, you will not have access to the whistleblowers' reports. Your role will be to perform platform configurations, support the organisation'sstaff receiving the whistleblowers' reports in their operation, as well as to establish best practices and ensure that every user implements them

To create a new user, click on *+Add* (1); you will be prompted to assign a role, and enter the user's username, name, and email address. Make sure the "*Send an account activation link to the user*" is ticked and click on *+Add* (2) to save.



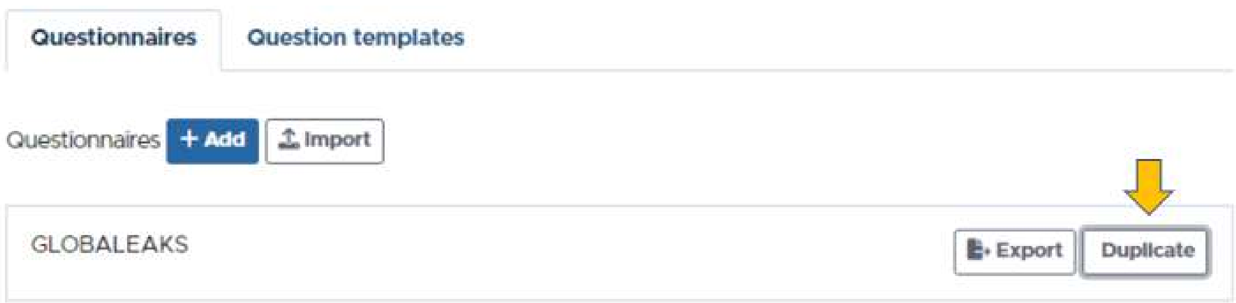
IMPORTANT NOTE

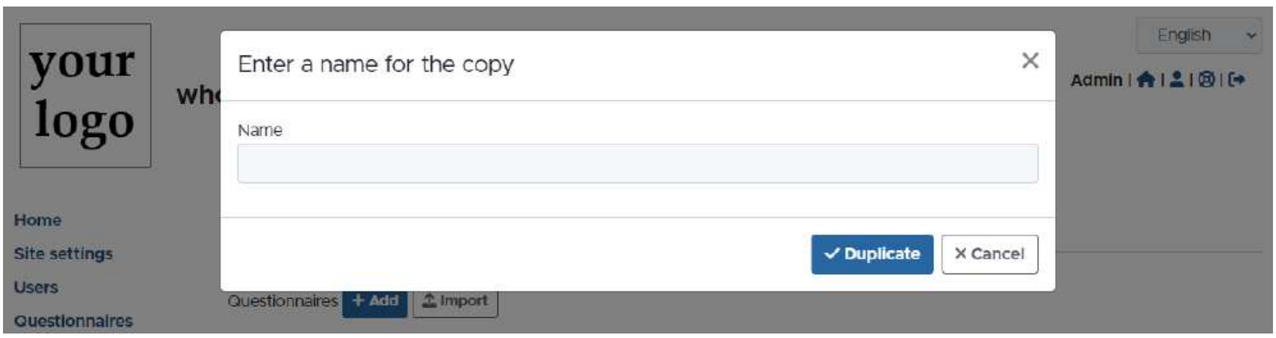
Please be mindful that **deleting Users** may result in **data loss**: by deleting a Recipient, **all reports** received by the specific user will also be **deleted**.

CONFIGURE THE QUESTIONNAIRE

The questionnaire should be adapted to the type of whistleblower that your organisation usually receives and/or seeks to attract.

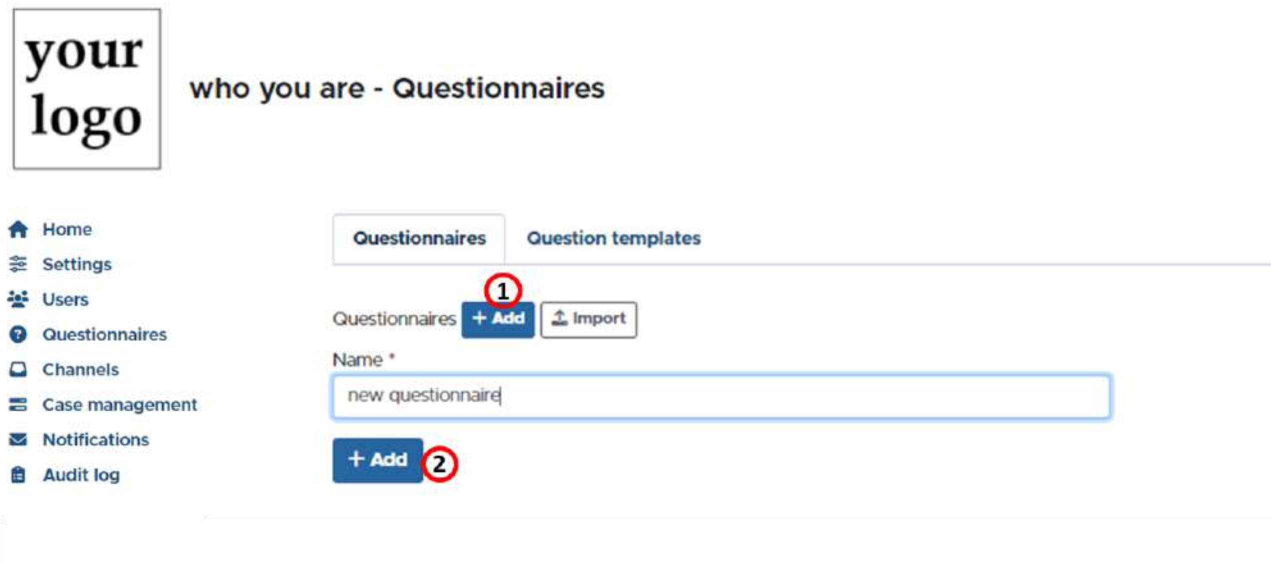
After the basic configuration is completed, the platform is configured with the GlobaLeaks Questionnaire, which is pre-associated to the Default Channel.
To edit the GlobaLeaks Questionnaire, you need to duplicate it; you will be prompted to enter a name for the copy, and you can then edit the questionnaire under the new name.





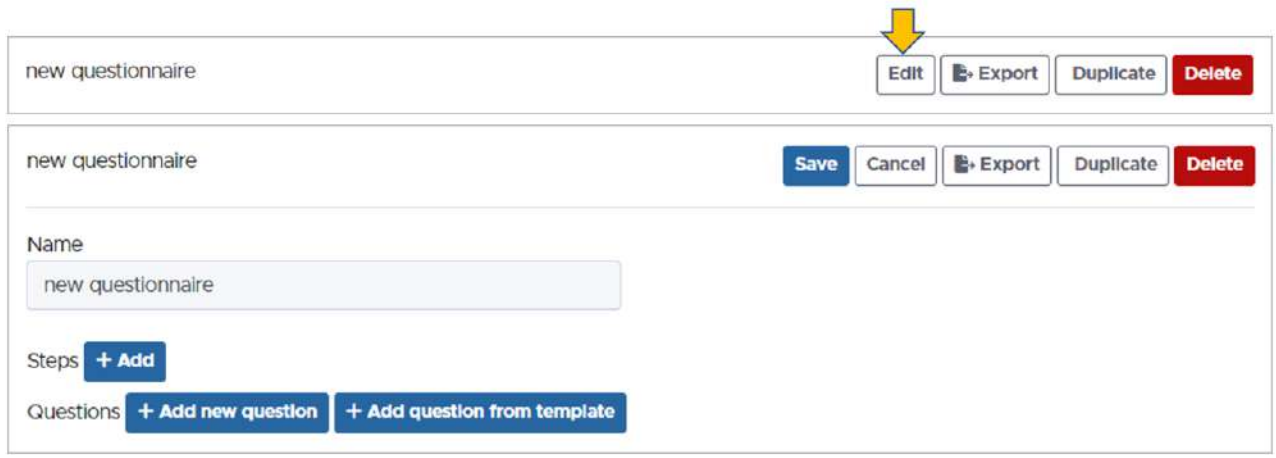
You can create Channel-specific questionnaires for each of your reporting channels (if applicable).

To create a new questionnaire without making use of the GlobaLeaks questionnaire, click on *+Add* (1); you will be prompted to give the questionnaire *Name*. Then click on *+Add* (2) to save.



After the new questionnaire is created, click on Edit to create the questions.

The platform offers the possibility to organize questions in steps (see below for more detail).



QUESTIONNAIRE STEPS

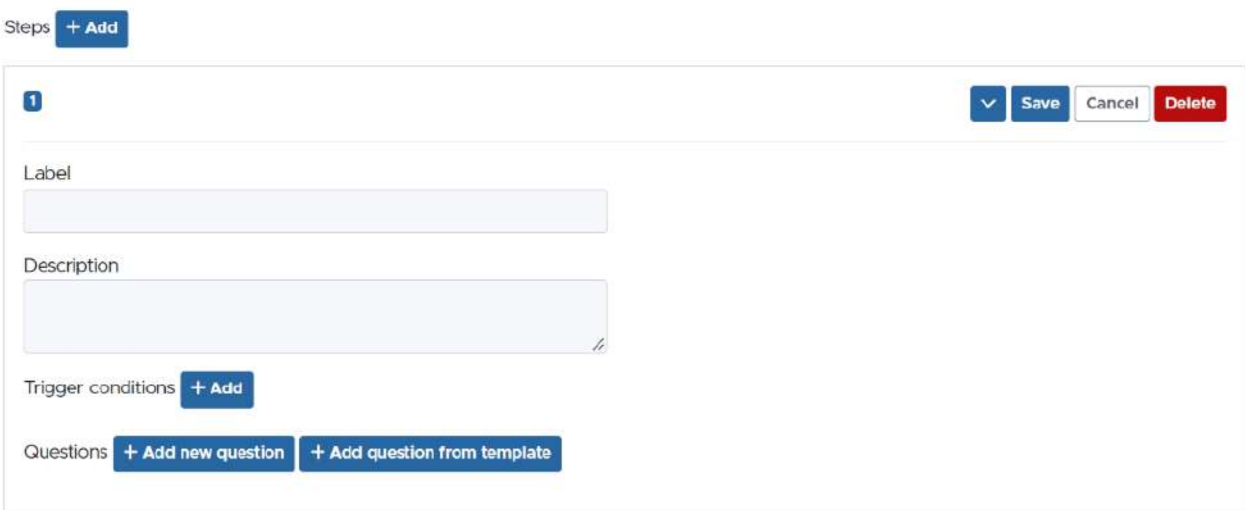
You can organize the completion of a questionnaire in one or multiple steps; that is, in different sections which will be separated on different pages.

The default questionnaire is organized with a single step including all the questions — whereas, for example, you could create a first step for the reporting person to read and agree to "Terms and Conditions", a second step for the "Report" set of questions, and a third step to collect data for statistical purposes (see examples below).

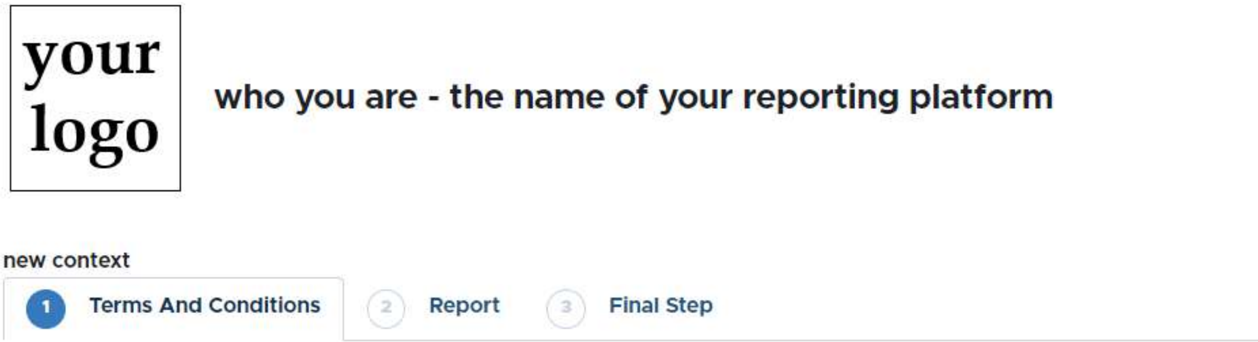
To create an extra step, click on *+Add* (1); you will be prompted to *Label* [name] the step, and then click on *+Add* (2) to save the new step.

After creating the extra step, you need to edit the steps:

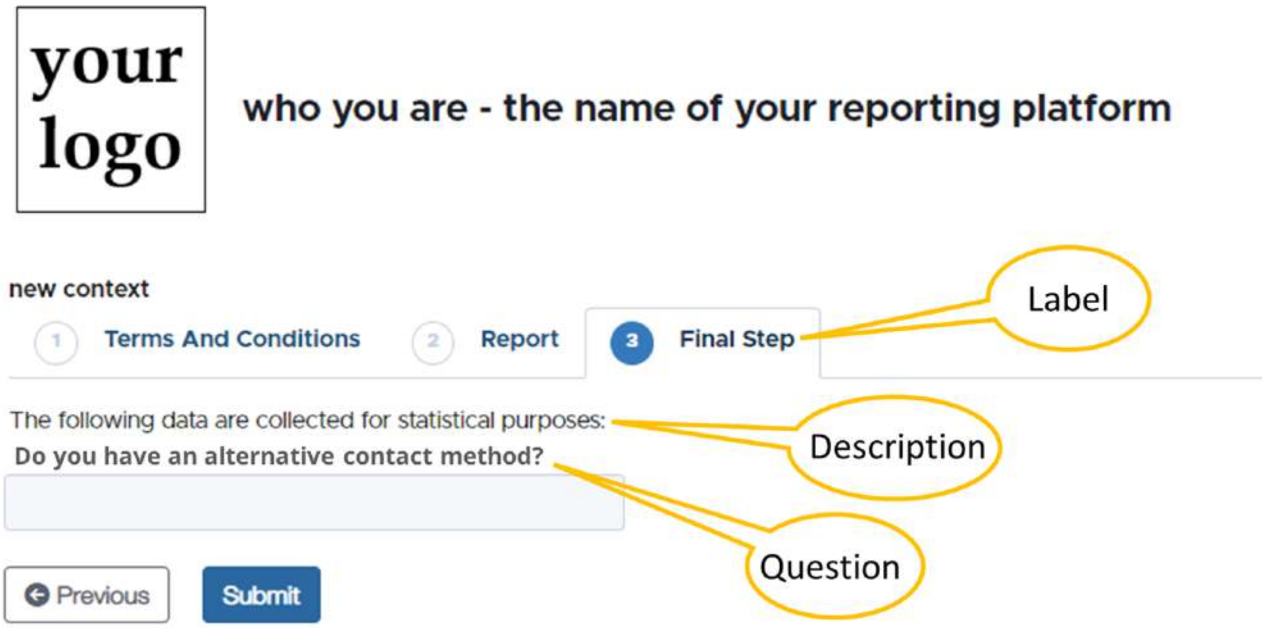
You can name (*Label*) the step, add a text to provide information for the step (*Description*), and add questions.



This is an **example** of what a questionnaire organized in three steps would look like:

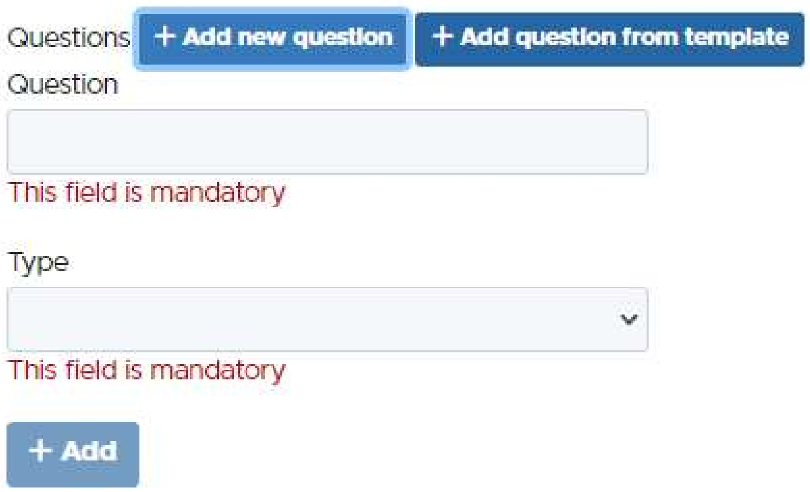


This is an **example** of what a step could look like after editing:

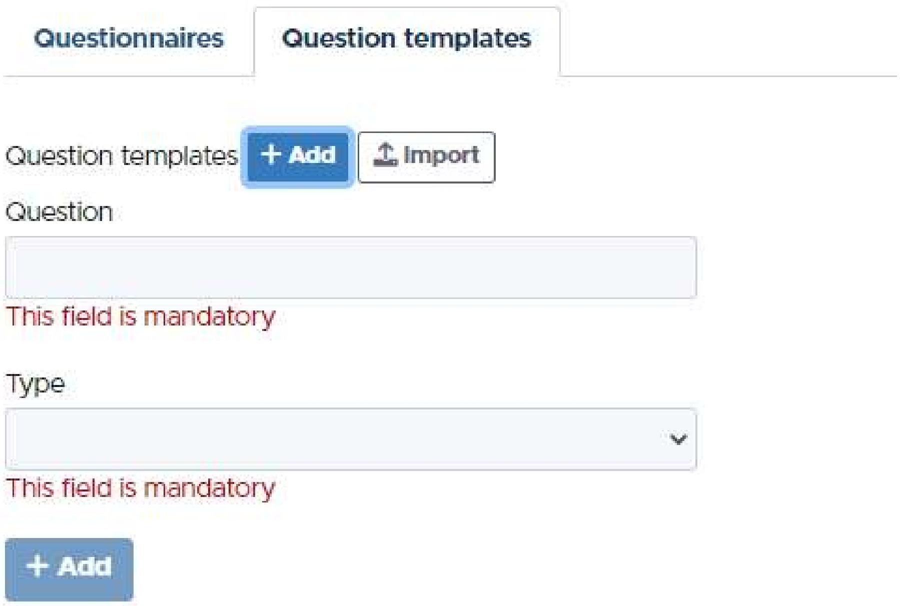


QUESTIONS

To create a question, click on *+Add new question*, type the question, choose the question type, and click *+Add*



***tip**: You can create questions either directly in the questionnaire, or as *Question Templates* in order to reuse them in multiple questionnaires.



- You can create questions of the following types:

Question types

Single-line text input

free text answer (by default limited to 100 characters)

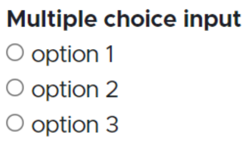
Multi-line text input

free text answer (by default limited to 2.000 characters)

Selection box

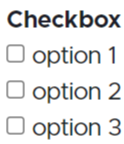
the reporting person will be able to choose only one answer from a drop-down menu

Multiple choice input



the reporting person will be able to choose only one answer

Checkbox



the reporting person will be able to choose more than one answers

Attachment

the reporting person will be able to upload files

Terms of service

the reporting person will be able to read and download a copy of the terms and conditions of the platform, and will be prompted to agree by ticking the checkbox

Date

the reporting person will be able to choose an exact date; you can set a specific period within which the reporting person can choose

Date range

the reporting person will be able to choose a start date and an end date

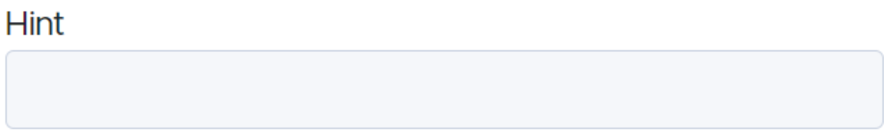
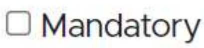
Group of questions

you can group related questions under a title

- After you have created a new question, you will need to edit it.
  For each question, and according to the question type, you can configure the following properties. Please note that you need to click on Save for each configuration!

Question Properties

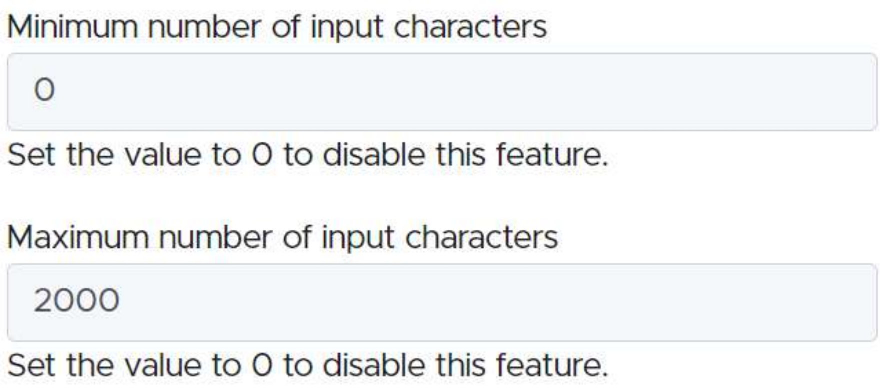
applicable to:
all question types

Name	Phrase your question
Type	Select question type (see above)
Hint	 Add a question mark next to the question to reveal a brief guidance/explanation via a popover text
Description	 Add a description text below the question
Mandatory	 Tick to set a field as required in order to proceed with submitting the report
Preview	 Tick to set this field if you want the Recipients (pre)viewing the answers to a question on their list of Reports
Width	 Set the width of the answer box

Question Properties

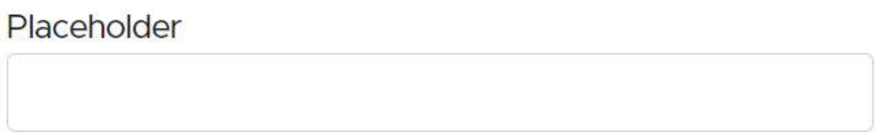
applicable to:
Single-line text input
Multi-line text input

Minimum/ Maximum number of input characters



Set the limitations for free text answers

Placeholder



Add an indication in the answer box (typically used to give the respondent an example)

Input validation

Define custom input validators by using regular expressions (ensures that data such as email address or phone number are entered in the correct format)

Question Properties

applicable to:
Selection box
Multiple choice input
Checkbox

For these three types of questions, you should offer the reporting persons multiple answer options to choose from. Also, these three types of questions offer the possibility to create associations between questions and answers, making different questions appear according to the reporting person’s answer to a previous question.

Example: question A is: *Is the report connected to your work?* and has two answer options for the reporting person to choose from: *Yes*, and *No*.

Options

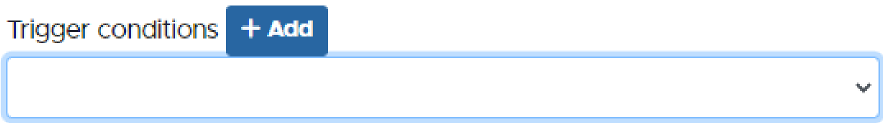
To create a set of answer options for a question, click *+Add* and type the answers; you can:

1. add/delete options,
2. change the order of options,
3. add hints to options (i.e. text to be shown after the reporting person has selected a specific option),
4. block the submission (e.g. if the reporting person’s choice indicates something the chapter cannot help with),
5. assign the report to specific recipients according to the reporting person’s choice

Example: If the reporting person's answer to question A *Is the report connected to your work?* is *Yes*, it will trigger question B to appear: *Do you have a valid employment contract?*

First, you would need to create question B.

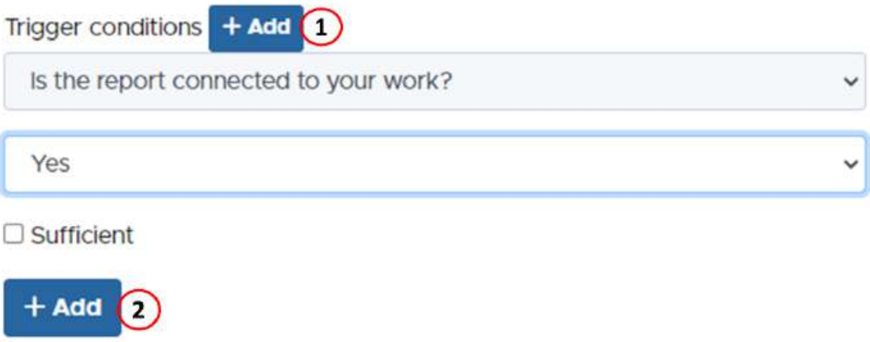
Then, you would need to edit it by adding Trigger Conditions:



Trigger conditions

Questions are displayed or remain hidden according to the reporting person responses.

To make the appearance of question B dependant on what the reporting person answers to question A, you need to create question B and then to edit question B: click on *Trigger conditions +Add (1)* and choose question A, and then choose the answer option(s) which will reveal question B; click on *+Add (2)* and click Save for question B.



If the answer to the question A is *No*, the question B will not appear.

To further the **example**, if the answer to question B *Do you have a valid employment contract?* is *Yes*, then it could trigger question C *Type of employment contract* with multiple choice input, in which all forms of contract would be listed (permanent contract of employment, temporary contract of employment, civil contracts, etc.) —you would need to create question C, and proceed to edit it by clicking *Trigger conditions +Add*, choosing question B and answer option "Yes"

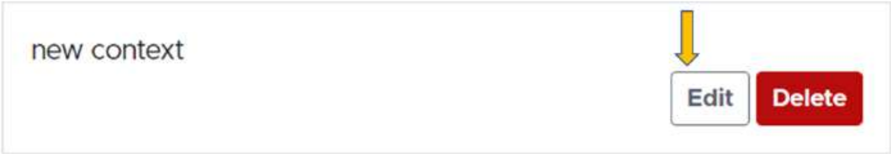
CONFIGURE THE CHANNELS [CONTEXT]

After the basic configuration is completed, the platform is configured with a single reporting Channel [Context], named "Default", which is associated with one Recipient and the default GlobaLeaks questionnaire. You can edit the default Channel – or create additional Channels and configure their respective recipients and properties, depending on your project requirements.

If you create more than one Channel, the reporting person will be prompted to select a reporting channel after clicking the "Report" button.

To create a new Channel, choose **Channels** from the menu on the left.

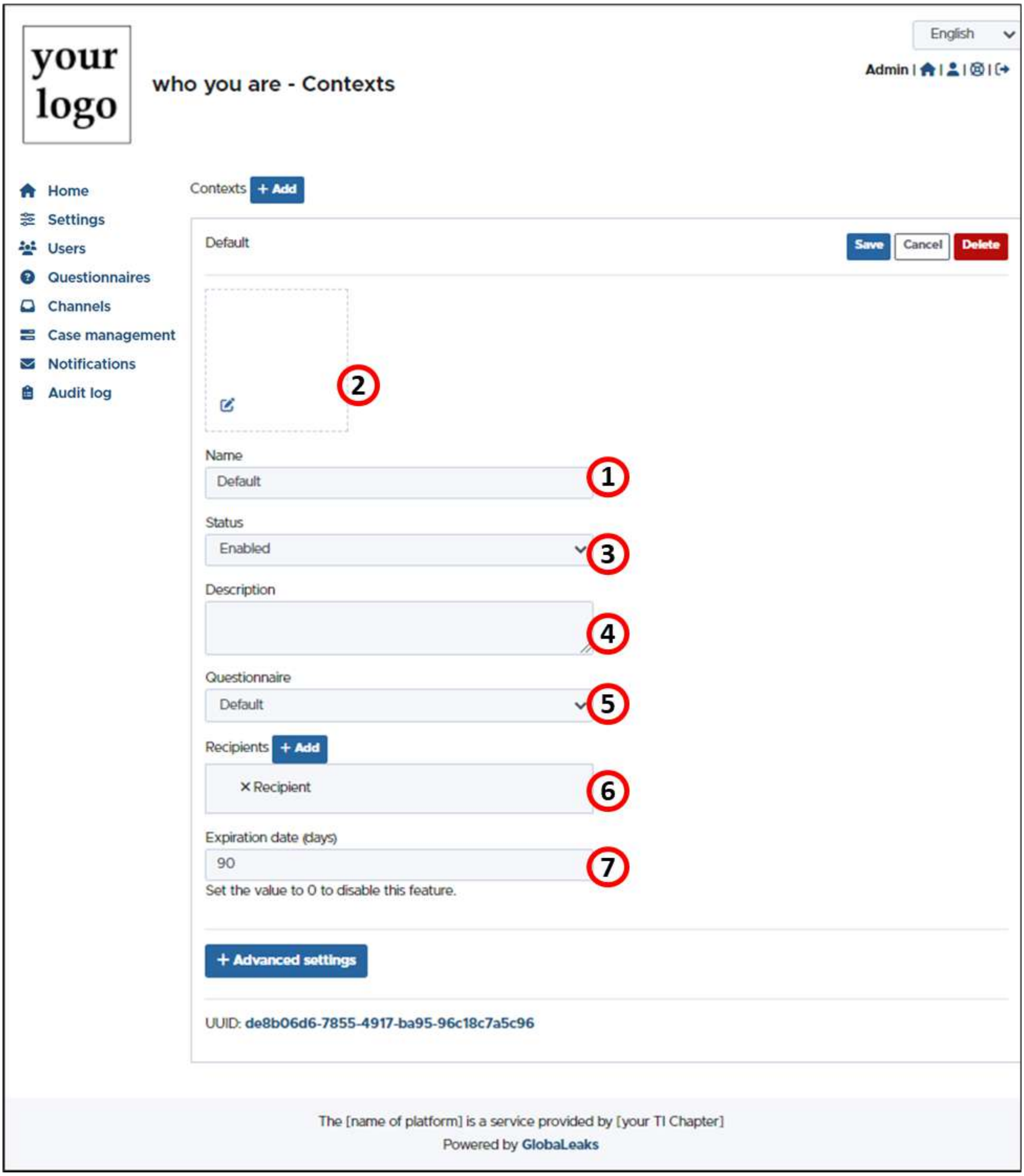
After the new Channel is created, you will need to edit it.



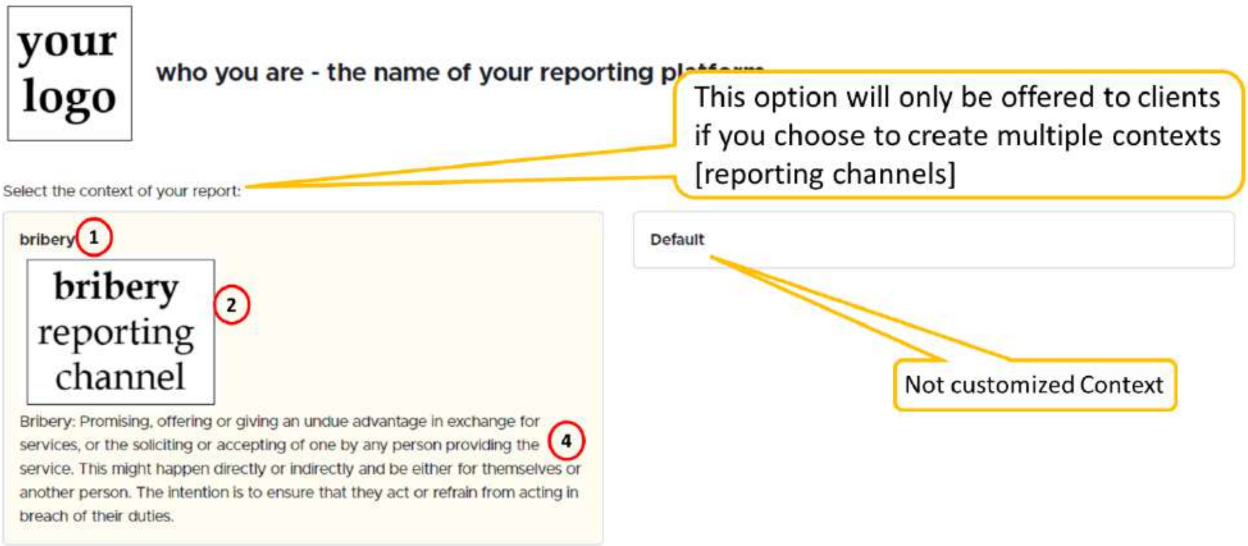
A reporting channel is defined by the following properties:
(also see in the image and example below)

Name: the name of the Channel
Image: an image/ logo to identify the reporting channel
Status: the reporting channel can be *Enabled*, *Hidden*, or *Disabled* (the reporting person will be able to access only the reporting channels in *Enabled* status)
Description: a description of the reporting channel
Questionnaire: the set of questions which the reporting person will be prompted to answer when selecting this reporting channel *
Recipients: the users who can access reports submitted through this reporting channel *
Submission expiration: the data retention policy for the reporting channel

> * the starred properties are required for the reporting person to be able to complete a report


English
Admin
your logo
who you are - Contexts
Home
Settings
Users
Questionnaires
Channels
Case management
Notifications
Audit log
Contexts
+ Add
Default
Save
Cancel
Delete
2
Name
Default
1
Status
Enabled
3
Description
4
Questionnaire
Default
5
Recipients
+ Add
× Recipient
6
Expiration date (days)
90
7
Set the value to 0 to disable this feature.
+ Advanced settings
UUID: de8b06d6-7855-4917-ba95-96c18c7a5c96
The [name of platform] is a service provided by [your TI Chapter]
Powered by GlobaLeaks

This is an **example** of what a customized channel could look like:



IMPORTANT NOTE

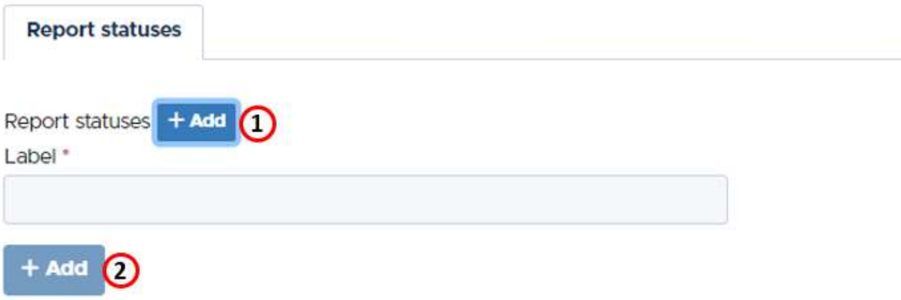
Please be mindful that **deleting Channels** may result in **data loss**: by deleting a Channel, **all reports** submitted through and stored in the specific Channel will also be **deleted**.

As a rule, please use the **red buttons** of the platform with caution, as they may result in **data loss.**

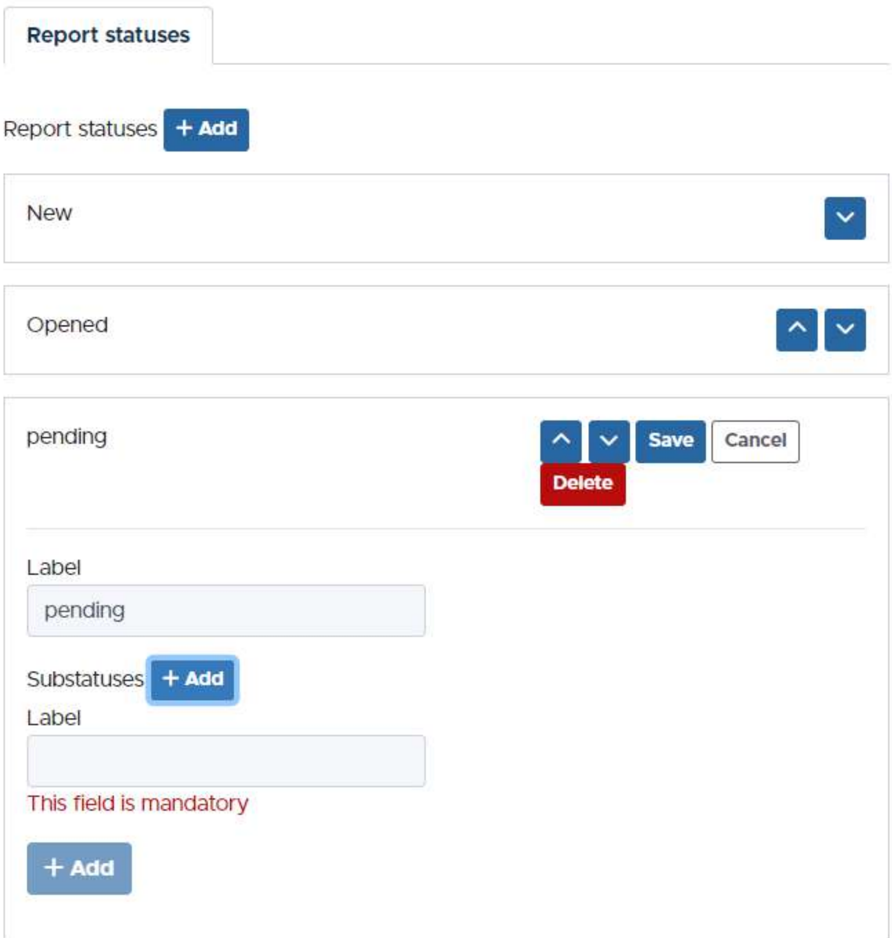
CONFIGURE THE CASE MANAGEMENT

When a Recipient receives a report, it is always set in “New” status. When the Recipient accesses the report, it is automatically set to “Opened” status, and cannot be set back to “New” —can only be set to “Closed” status.

According to your project workflow and requirements, you can add intermediate statuses.



After the custom status is created, you can edit it to add sub-statuses.



III. NOTES ON OPERATIONAL SECURITY

Please be mindful that operating a system which allows you to communicate with reporting persons may also attract viruses, malware, and other online threats. In case a virus attacks a recipient's computer, not only could it damage said computer, damage files, and result to data loss, but it could be transferred to and affect your entire computer network. Therefore, we urge you to have a cybersecurity policy in place.

> Please note that, while downloading a file from GlobaLeaks is safe, opening a file which contains malware may affect the recipient's computer, as well as the entire network the affected computer is connected to. Please consider putting in place an **advanced cybersecurity measure** such as an air-gapped computer, i.e., a computer that is not connected to the internet (neither physically, nor wirelessly) and is isolated from your network, in which data can only pass via removable storage media (e.g., USB). Recipients would download the report attachments on their computer, but then transfer, open, and examine them on the air-gapped computer.

BASIC SECURITY RECOMMENDATIONS

- Ensure that recipients' computers are protected by an Antivirus software; consider installing a commercial, subscription-based antivirus software package and update it regularly.
- Encrypt recipients' computers; please consider running an up-to date professional edition of Windows (currently Windows 10 or 11 Pro), to enable the BitLocker feature in order to prevent data breaches in case recipients' computers get stolen or lost.
- Have a password protection policy in place: password protect recipients' online accounts and data.
- Ensure that recommendations to whistleblowers are in place regarding the use of Tor Browser. The Tor Browser will protect their anonymity and hide their online activity.[6]
- The GlobaLeaks software does not protect against environmental factors related to users' physical locations and/or their social relationships. For example, if a user has a video bug installed in their house to monitor all their activity, GlobaLeaks cannot protect them. Likewise, if a reporting person, who is supposed to be anonymous, tells their story to friends or co-workers, GlobaLeaks cannot protect them.

[6] https://www.torproject.org/

RECOMMENDED ADVICE TO RECIPIENTS

As an Administrator, you should not only provide technical support for/to the organisation's staff receiving the whistleblowers' reports but also establish best practices and ensure that every user implements them. Please consider conveying the following advice to recipients:

Opening attachments from unknown sources may carry an element of risk.

- Please note that, while downloading a file from GlobaLeaks is safe, opening a file which contains malware may affect your computer, as well as the entire network your computer is connected to.
- Please be careful when opening report attachments. Firstly, read the whistleblower answers to the questionnaire carefully and assess the legitimacy of the report. In case of doubt, make sure to reach out to your colleagues and/or team leader. Attachments in reports that do not seem plausible or legitimate could pose a threat; thus, the risks of opening them should be weighed in.
- When it comes to sharing information you received with colleagues, it is advisable not to forward the original attachment as received in the report, but rather to share a summary of the most relevant information. In case you need to share an entire attachment, make sure to check before sharing a potentially malicious file online and put your computer network at risk.
- On a relevant note, replicating documents by taking screenshots or copying text into a new document, printing and re-scanning it into your computer is considered a good practice to avoid sharing metadata; metadata is data hidden in data to characterize it. All digital files contain metadata about the who, what, when, where, why, and how about every aspect of the file and can expose information traceable to the source of the file.[7]

Did you know there is a way to remove hidden data and personal information from a document in Microsoft Word?

1. **File > Info > Check for Issues > Inspect document**
2. **Document Properties and Personal Information**
3. **Remove All**

[7] If you are comfortable using more advanced software tools, please find information about managing metadata here: [Everything you wanted to know about media metadata, but were afraid to ask (freedom.press)]

Before using the GlobaLeaks software:

- Ensure that your computer's Antivirus software is enabled and updated. Use the AV to scan the files attached to reports.
- Encrypt your computer; if you are using Windows, ensure you have a Professional license and enable the BitLocker feature. If you are using other operating systems, please follow your platform Administrator's advice on this topic. Hardware encryption can help prevent data breaches in case your computer is stolen or lost. Encrypting your computer's drive means that, to start up the PC, you need to use a password.
- Password-protect your computer by setting a strong password to secure your user account and data (this is an additional method of authentication, different from the encryption start-up password). Combine words that would not normally go together and replace some of the letters with numbers and similar-looking special characters to create a long and complicated password; store your password in a safe place without any indication of what it is; change your password regularly; consider using a password manager app to securely manage and store your passwords (e.g., KeePassXC).