ODIHR Hate Incident Reporting Platform

User’s Manual

Table of Contents

1. Overview

The main purpose of the platform is to allow people who experience hate crimes or other incidents as either victims or witnesses to submit reports to trusted civil society organizations (CSOs) and for CSOs to monitor hate crimes and other incidents that they find important for their activities. The software has a secure back-end available only to registered CSO staff and is designed to manage, classify and keep track of reports received.

The hate incident reporting platform is using a Hypertext Preprocesssor[1] (PHP) application that is easily configurable via configuration files. The platform runs best on 64-bit Linux distributions like Ubuntu or Centos.

The platform uses cookies that enable a user session. They track:

- What page the user is on;
- The user's last actions;
- The user's language preferences.

These cookies are deleted after each user session.

2. Structure

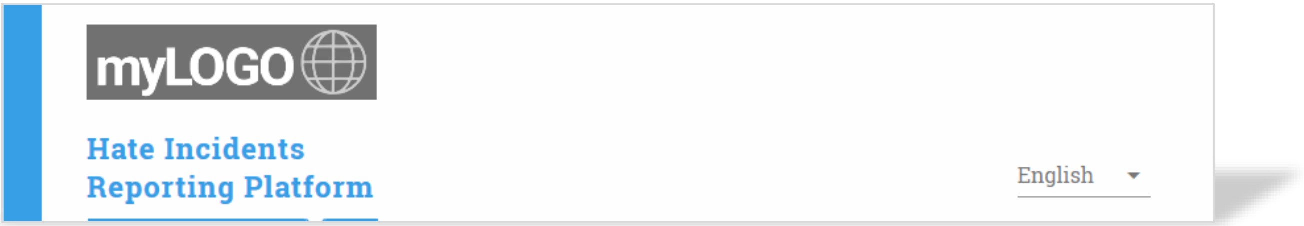
The platform is a set of two applications:

a. Front-end: The website is available for everyone that uses the reporting form, and contains static pages with information about the designated CSO, their contact data, details about privacy policy and a FAQ. It allows people to submit reports about hate crimes or other incidents and they can do so anonymously if they choose.

b. Back-end: The website is available only for users created by the designated IT administrator. The purpose of this application is to handle incoming reports by assigning them to certain users who can then classify the reports and take note of every action related with a particular incident.

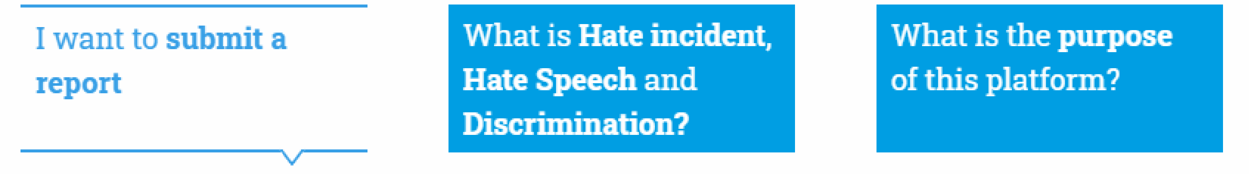
2.1. Front-end Application Layout

Header section – contains a customizable logo, the platform's name, and a language switch.

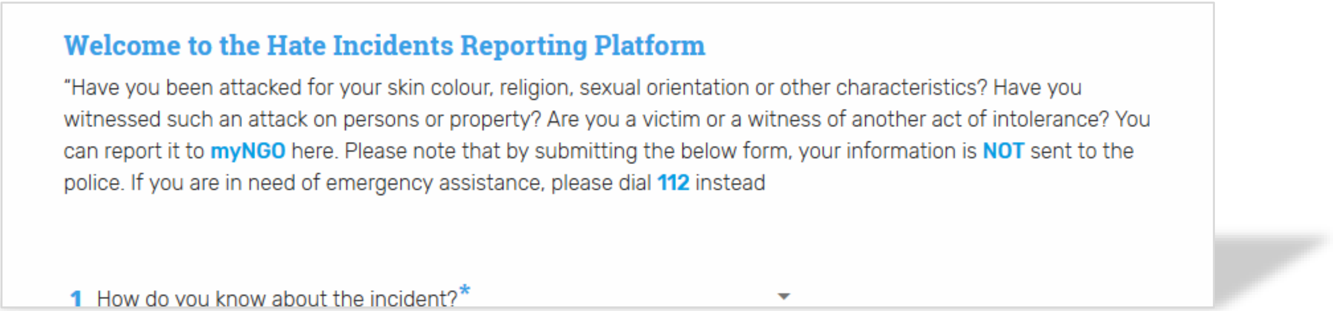


[1] PHP: Hypertext Preprocessor or simply PHP is a general-purpose programming language used for web development.

Navigation section – allows switching between the three most important pages.


I want to submit a report
What is Hate incident, Hate Speech and Discrimination?
What is the purpose of this platform?

Content section – contains page contents.

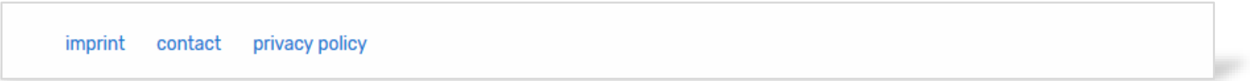


Welcome to the Hate Incidents Reporting Platform

"Have you been attacked for your skin colour, religion, sexual orientation or other characteristics? Have you witnessed such an attack on persons or property? Are you a victim or a witness of another act of intolerance? You can report it to **myNGO** here. Please note that by submitting the below form, your information is **NOT** sent to the police. If you are in need of emergency assistance, please dial **112** instead

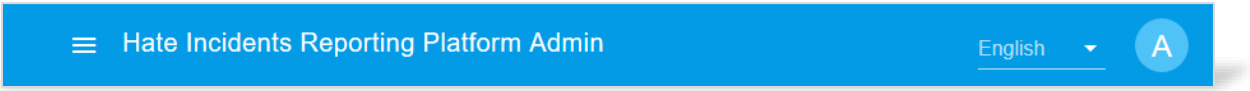
1 How do you know about the incident?*

Footer – contains links to static pages.

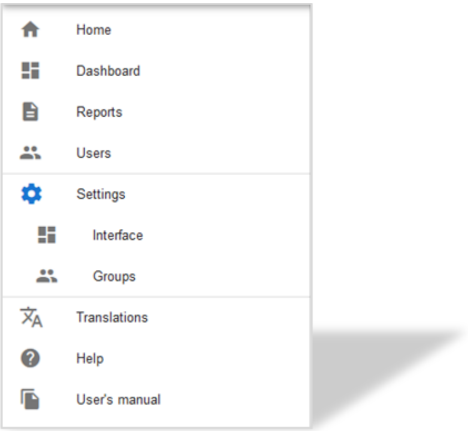


2.2. Back-end Application Layout

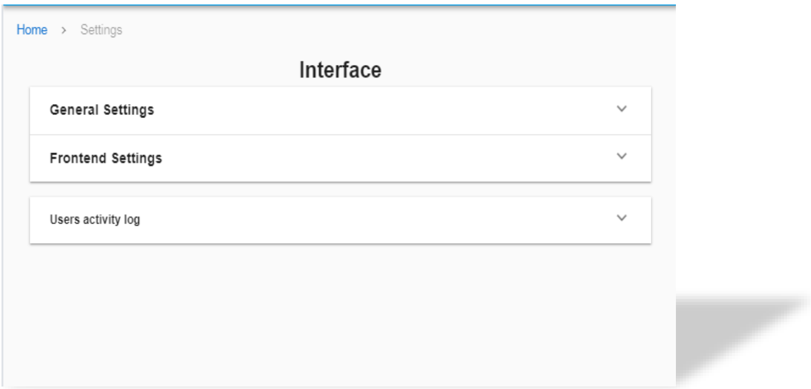
Header – contains menu toggle, name of the platform, language switch and a link to the user profile section.



Menu – lists functions available to user.



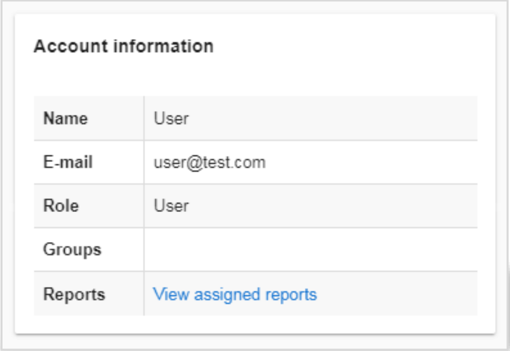
Content section – displays selected function.



3. Dashboard

The dashboard is individual for every user. It displays a summary of key information about the user, their recent actions and a list of reports assigned to them.

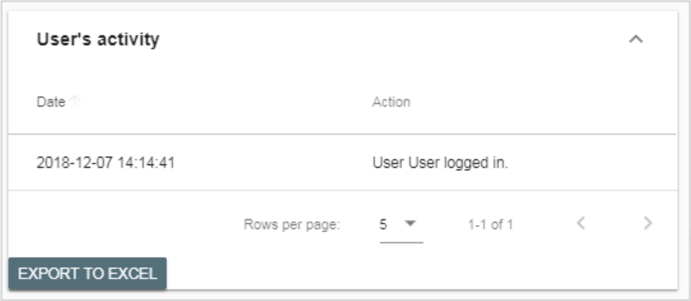
The account information section is on the top left corner of the page. It displays the key information about the user and contains a link to the list of reports assigned only to this particular user.



Account information

Name	User
E-mail	user@test.com
Role	User
Groups	
Reports	View assigned reports

The user's activity section is on the top right section of the page and contains a list of the actions the user has taken on the platform. This list of actions can also be exported to Excel.

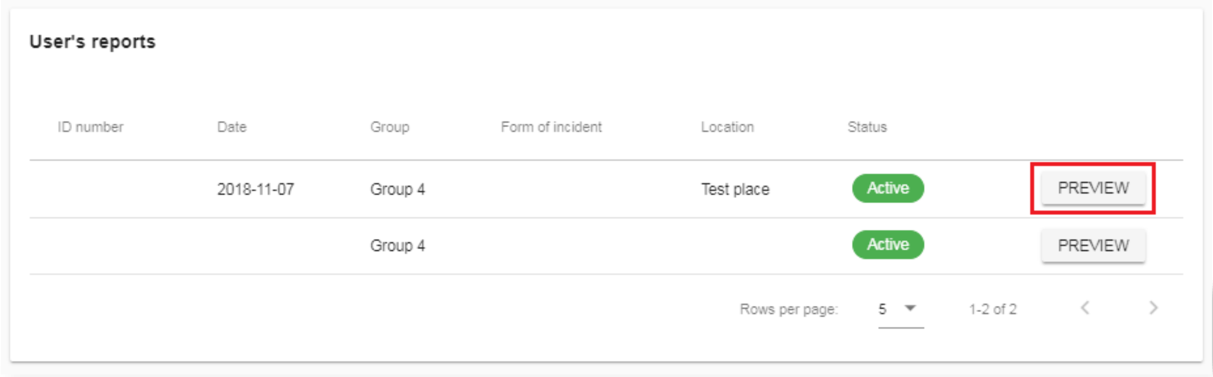


User's activity

Date	Action
2018-12-07 14:14:41	User User logged in.

Rows per page: 5 1-1 of 1

The bottom section of the dashboard contains a list of reports assigned to the user. The user can click the 'Preview' button to view each report in more detail.



User's reports

ID number	Date	Group	Form of incident	Location	Status	
	2018-11-07	Group 4		Test place	Active	PREVIEW
		Group 4			Active	PREVIEW

Rows per page: 5 1-2 of 2

4. Reports

The reports come into the database (back-end application) from two main sources:

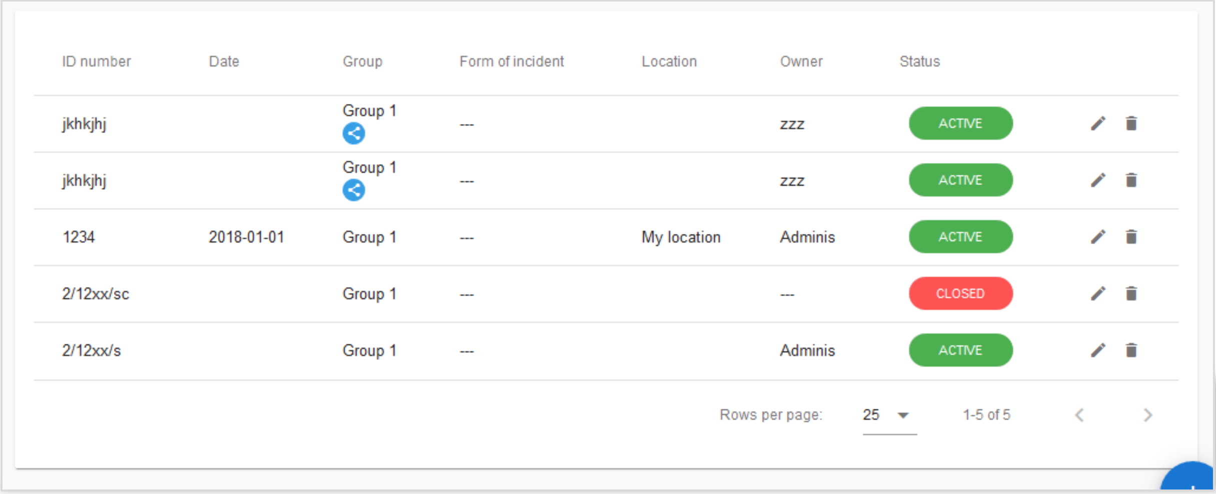
- They are reported through the front-end application by external users (victims or witnesses of incidents);

- They are entered into the database through the back-end application by registered users (CSO staff). These reports can be incidents reported to the CSO on the phone, in a conversation or spotted in the press.

All reports appear on the same list of reports available after clicking on the ‘Reports’ section on the menu bar.

4.1. Navigating the Reports List

The reports list contains all incidents available for a particular user. The number of incidents may differ depending on the user role, group membership and current filter settings. The reports list as well as other lists in the back-end application has features that make browsing easier, such as column sorting or pagination with adjustable number of items per page.



ID number	Date	Group	Form of incident	Location	Owner	Status	
jkhkjhj		Group 1	---		zzz	ACTIVE	✎ 🗑
jkhkjhj		Group 1	---		zzz	ACTIVE	✎ 🗑
1234	2018-01-01	Group 1	---	My location	Adminis	ACTIVE	✎ 🗑
2/12xx/sc		Group 1	---		---	CLOSED	✎ 🗑
2/12xx/s		Group 1	---		Adminis	ACTIVE	✎ 🗑

Rows per page: 25 1-5 of 5

Actions Available on the List of Reports

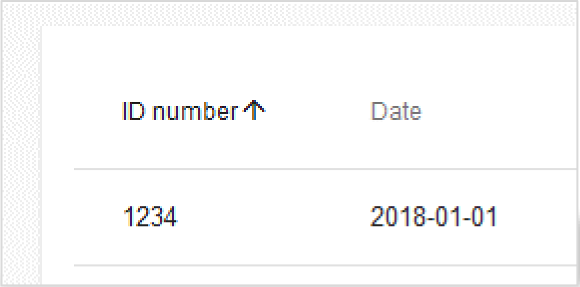
For each report on the list the user can perform the following actions:

- **Edit report** by clicking the pencil icon ✎
- **Delete report** by clicking the rubbish bin icon 🗑
- **Change status** between ACTIVE and CLOSED by clicking on the status indicator.

Sorting

Most columns can be sorted. By default the incidents are sorted based on the date they were entered into the database. There are three states of column sorting:

- Default - arrow may not be displayed or is dimmed ↑ when sorting of a selected column is turned off and default sorting takes place;
- Ascending - when set arrow pointing up ↑ appears next to column name;
- Descending - when set arrow pointing down ↓ appears next to column name.

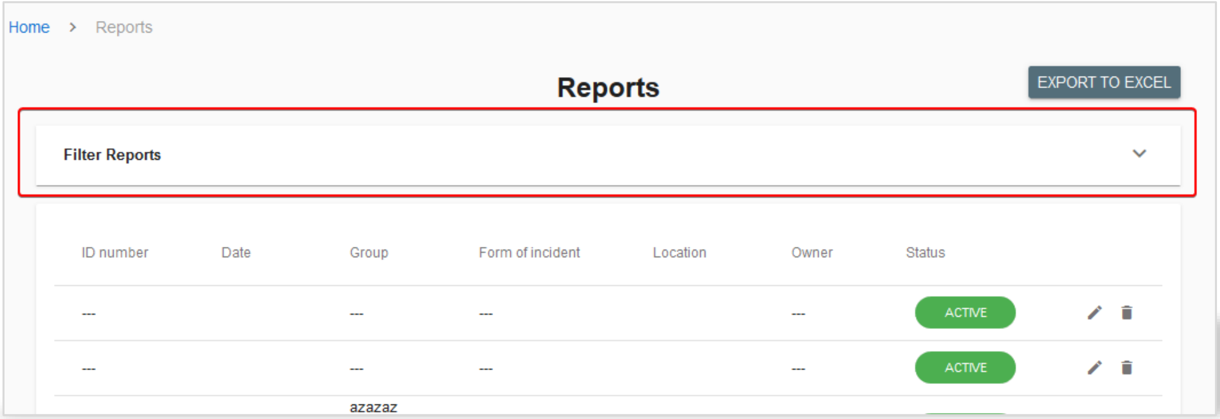


ID number ↑	Date
1234	2018-01-01

4.2. Filters

The users can view the list of incidents that are available according to their respective role. The report list allows for filtering and sorting of incidents according to users' needs.

The filter section is located above the reports list and can be expanded by clicking on it.



Home > Reports

Reports

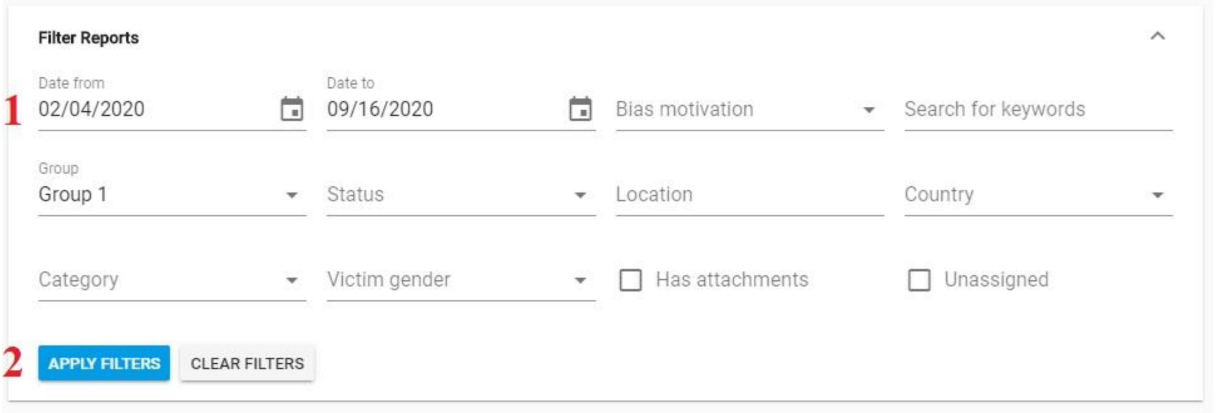
EXPORT TO EXCEL

Filter Reports

ID number	Date	Group	Form of incident	Location	Owner	Status
---		---	---		---	ACTIVE
---		---	---		---	ACTIVE
		azazaz				

In order to set the filter, (1) fill one of the control bars and (2) press APPLY FILTERS button. The list below should be reloaded immediately.

If you would like refine your search, fill additional control bars and click APPLY FILTERS again. If you would like to start a new search, click CLEAR FILTERS and set up new search criteria.



Filter Reports

1 Date from: 02/04/2020
Date to: 09/16/2020
Bias motivation
Search for keywords

Group: Group 1
Status
Location
Country

Category
Victim gender
□ Has attachments
□ Unassigned

The incidents can be filtered by:

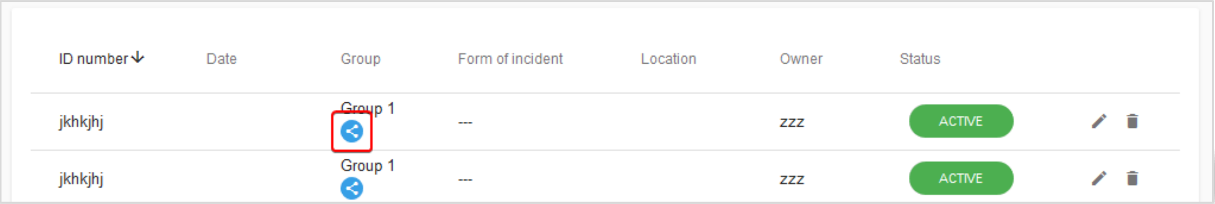
- Date;
- Bias motivation;
- Group;
- Status;
- Location;
- Country;
- Incident category;
- Gender of the victim;
- Whether or not it has attachments.

The keyword search bar allows searching the contents of the reports based on any words that appear in any part of any report. An additional filter for 'unassigned' incidents is available for administrators and content administrators to facilitate the assigning of incidents to specific groups or users.

4.3. Shared Reports

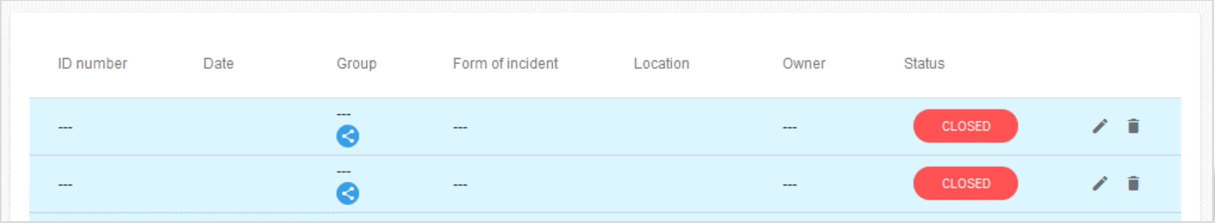
The incident reports can be shared between and among groups. Sharing makes the report visible to members of other groups to preview and print. If an incident is shared with another group, it will be marked with a blue icon for regular users and with a ‘Share’ icon for the administrators. The administrators can hover the mouse over the icon to quickly preview with whom the incident is being shared. For more information on how to share reports with other groups, go to section 5.2.

The display of the list with shared incidents for content and group administrators:



ID number↓	Date	Group	Form of incident	Location	Owner	Status
jkhkjhj		Group 1	---		zzz	ACTIVE
jkhkjhj		Group 1	---		zzz	ACTIVE

The display of the list with shared incidents for a regular user:

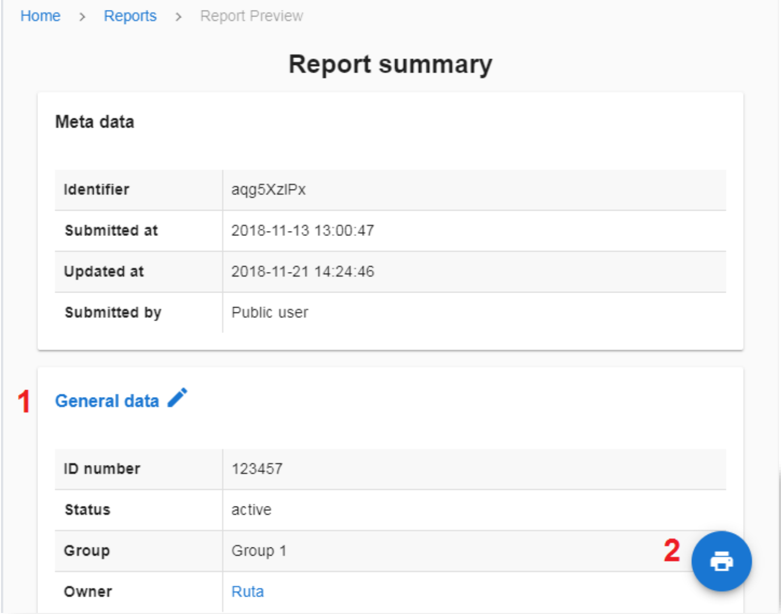


ID number	Date	Group	Form of incident	Location	Owner	Status
---		---	---		---	CLOSED
---		---	---		---	CLOSED

4.4. Preview and Print

The user can preview each report in more detail by clicking on any of the listed information. This takes the user to a ‘Report summary’ page of individual reports. All information about a given report is displayed on this page. To protect sensitive private data, the displayed information varies depending on the user role.

To edit the report, click on the highlighted blue headings (1). To print the report, click on the print button on the bottom right-hand corner of the report summary page (2).



Home > Reports > Report Preview

Report summary

Meta data

Identifier	aqg5XzlPx
Submitted at	2018-11-13 13:00:47
Updated at	2018-11-21 14:24:46
Submitted by	Public user

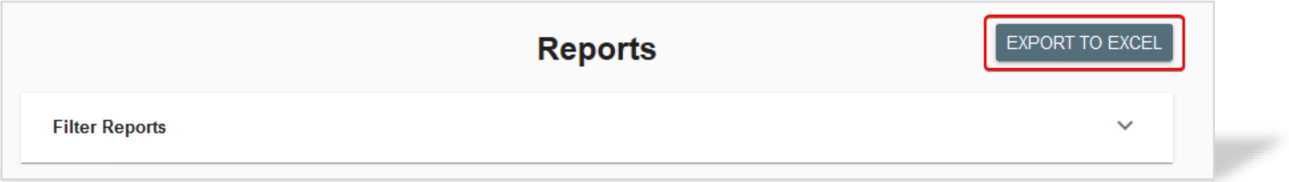
1 General data

ID number	123457
Status	active
Group	Group 1
Owner	Ruta

2

4.5. Exporting Reports

The list of reports can be exported to Excel by clicking on the 'EXPORT TO EXCEL' button placed over the 'filters' control. The incidents exported to Excel will depend on the user's role, group, and the filters applied at the time of the export.



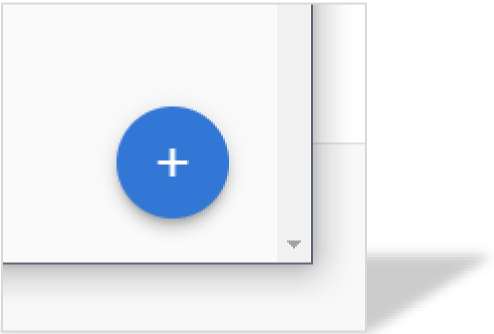
After clicking the export button, a pop-up window will appear which will prompt you to select the data categories you would like to export. You can either select all categories at once or pick the specific categories that you require for the purpose of the export. The selected categories will appear as columns on an Excel sheet.

Point of caution! If you are exporting the data for statistical purposes or for sharing, you should not export the reporter's personal data or any other sensitive information.

5. Creating and Editing Reports

5.1. Creating New Reports

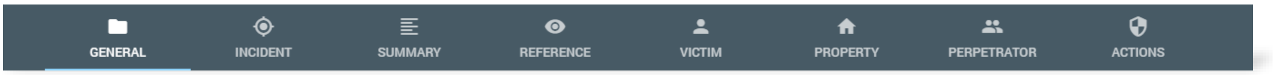
In order to create a new report, go to the list of reports and click on the '+' icon placed in bottom right corner of the screen. The report form is available to all types of users apart from the guests, but user's access to certain fields in the form may be limited depending on their role.



5.2. Report Form Sections

The same form is used for editing the reports received through the front-end application and for newly created reports.

On the top of the page, the report editing form has a navigation bar, which allows users to switch between the sections of a given report. The users can review and edit information in these sections.



General Section

ID number – This is a text field.[2] Any characters are allowed in this field. However, the inserted ID number has to be unique. If a value that is already used is provided, an error message appears and it becomes impossible to submit the form. This section is intended for CSOs to use a system of numbering that is convenient for them. ID numbers are different from automatically generated 'Identifiers.'

Owner – This is a drop down field.[3] Each report can have an individual user responsible for it. Being an owner of an incident allows the user to access the reporter's contact details, which are otherwise available only to administrators. The number of users displayed on the list can be limited by selecting 'Group' first.

Group – This is a drop down field. This field allows assigning an incident to a group, which will be responsible for managing the incident in the future.

Status – This is a drop down field. There are two status options: 'Active' and 'Closed'. The status is only used to signal to users if additional actions are necessary. It does not affect the information in the report or related functionalities.

Share with group(s) – This is a drop down field with tick boxes.[4] The option allows sharing incidents among different groups. A given report can only be assigned to a single group, but can be shared with other groups. The groups with which the report is shared can view the information in the report but cannot edit it.

Incident Section

Date – This is a calendar field which allows users to select the date on which the incident took place.

Location – This is a text field. The user is free to provide any location related information. The section can be connected to Google location services, allowing for the storage of information about exact locations of the incidents.[5] Otherwise, if the CSO choses, the location information can be limited to the town or a description

Country – This is a dropdown list of countries. In order to quickly select the country in which the incident took place the user can start typing the name of the country.

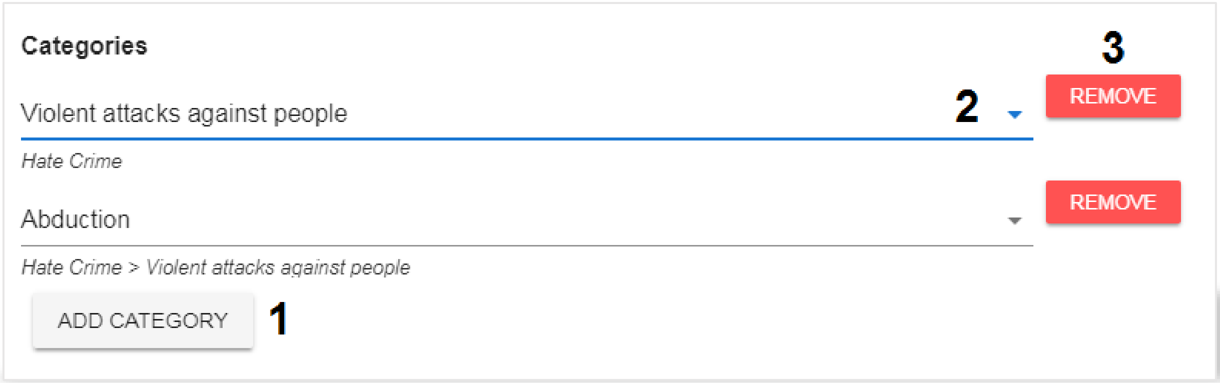
Categories – This field allows users to classify the incidents by the type of offence. To add a category to an incident, click 'Add category' then select a category from a drop-down list of categories (2). To remove a category click the red 'Remove' button (3). Each incident can be ascribed multiple categories which is useful when the incidents involve different offences.

[2] 'Text field' means that the users can enter any text into a provided field.

[3] 'Drop down field' means that the user can choose one out of many options that appear after clicking on the field.

[4] 'Drop down field with tick boxes' functions the same way as a drop down field, but allows the user to select multiple options, by ticking the box displayed next to each option.

[5] It is important to know that Google services uses cookies to track user behaviour both in the publicly available reporting form and in the back-end. Therefore, in countries where compliance with the GDPR is compulsory it is advisable to disable Google location service.



Categories

Violent attacks against people

Hate Crime

Abduction

Hate Crime > Violent attacks against people

Bias motivation – This is a list of bias motivations with multiple choice tick boxes. You can tick the boxes with the matching bias motivation. Multiple bias motivations can be marked. There is a text field at the bottom of the section for additional notes.

Indicators of bias motive – This is a list of tick boxes and after ticking each box a text field for more information appears. There can be multiple indicators of bias motives.

Summary Section

Summary – This is a text field. It may contain larger descriptions of incidents. This field contains the incident description which the reporter submits through the front-end reporting form. The edits in this section should be minor and aimed to only ensure that no sensitive private data is stored on the platform unlawfully. Therefore, only IT, content and group administrators can edit this field. As the field contains the information submitted by the external users it may contain sensitive information about the reporter or third parties. The content administrator should review this field carefully and depending on the type of sensitive data,[6] chose either to delete the sensitive data permanently or to anonymize it by putting two underscores ('_' symbol) before and after the section he or she wishes to anonymize. For example: *Witness name is __John Doe__*. Such anonymization will leave the sensitive data available for the content administrator, but display this to other users as: *Witness name is* **[RESTRICTED INFORMATION]**. Removing the underscores will disclose the information to all users.

The field also contains an additional text tab 'For cases added by the CSO users' to provide a user an opportunity to add a case description in case an incident was added by a user through the backend

Reference Section

Information on the reporting person and process – This is a text area field. It may contain larger descriptions of information. If you would like to add comments or additional information about specific incidents, it is advisable to insert such information here.

Upload file – If a file was uploaded by the reporter through the front-end it will be displayed here. The users will be able to download and view these files. The users can also upload additional documents in the following formats: .doc, .docx, .xls, .rtf, .txt, .pdf, .jpeg, .jpg, .bmp, .png, .gif.[7] The maximum file size allowed is 20 megabytes. Multiple files can be uploaded at once.

[6] In most cases the sensitive data on the platform will be processed on the legal basis of the explicit consent of the data subject. Incident summaries may include information about third parties but only the reporter may provide consent to process their private data. In situations when summaries mention third parties, the content administrator should consider whether the data allows identifying these third party individuals.

[7] When uploading the files, it is important to bear in mind that when data is processed on the basis of consent, files may only contain information about people whose consent has been obtained.

Reporter contact agreement – This is a checkbox. If a reporter (through an online reporting form) is a witness or other, this checkbox will be checked automatically.

Special remarks for the contact – This is a text area field for any remarks.

Victim Section

Age – This is a numeric field. It should indicate the victim's age.

Nationality – This is a text field. Users can insert information about the victim's nationality, if known or relevant.

Gender – This is a dropdown field. The 'Other' option allows for specifying information about the victim's gender in the special text field that appears next to the gender section.

Origin – This is a text field. It allows the users to insert information about the victim's ethnic identity if known or relevant.

Further information – This is a text field for further information.

Relevant markers of victim identity – This is a text field. It allows inserting information about the markers of the victim's identity. Markers of the victim's identity can serve as bias indicators and help prove that the crime or the incident was motivated by bias.

Harm suffered – This is a text field. It allows inserting information about the physical or psychological harm suffered by the victim.

Assistance needs – This is a text field for inserting information about the victim's assistance needs.

Victim contact agreement – This is a checkbox. If a reporter (through an online reporting form) is a victim, this checkbox will be checked automatically.

Property Section

Property information – This is a text field. In case the incident falls into the category of attacks against property, additional information about the type of property can be inserted here. If the property is marked in specific ways that signifies its belonging to a particular ethnic or religious group, this information can help prove that the incident was motivated by bias.

Damage – This is a text field. It provides space for inserting information about specific damage done to the property.

Perpetrator Section

Committed by a – This is a dropdown field, this section allows choosing whether the incident was committed by an individual perpetrator or a group. Remember that perpetrator's belonging to a known hate group can serve as an indicator of bias motivation.

Committed by law enforcement – This is a single checkbox.

Relevant perpetrator information – This is a text field. Use this space to note any relevant information about the perpetrator. This section should be used with caution given concerns around data protection. It is not likely that the perpetrator will have given explicit consent to process their private data.

Actions Section

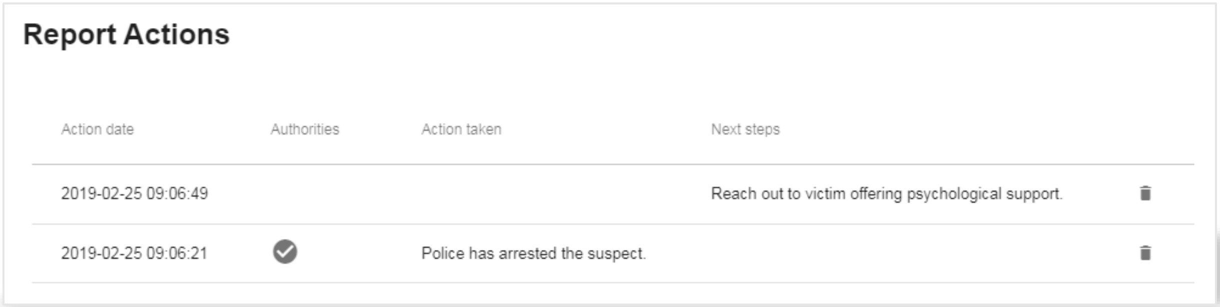
This section is available only after the report has been saved in the system and can be used for follow-up activities or leaving notes to colleagues. It allows registering multiple actions taken by the CSO, individual staff members or public authorities. After adding the first action, a table of registered actions will be shown with the option to sort or remove the previously added actions. It is possible to add separate actions or necessary next steps. The ticking of boxes allows for distinguishing the actions taken by the authorities from the actions taken by the CSO's staff.

Actions Section Form Fields

Action taken – This is a text field for filling in the actions that have been taken.

Next steps – This is a text field for filling in the information about planned or requested actions.

Action taken by authorities – This is a checkbox. It allows marking any actions taken by the authorities.



Report Actions

Action date	Authorities	Action taken	Next steps
2019-02-25 09:06:49			Reach out to victim offering psychological support.
2019-02-25 09:06:21	✓	Police has arrested the suspect.	

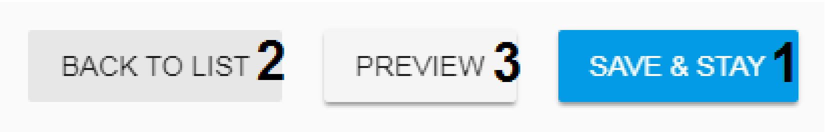
5.3. Submitting and Saving Reports

The 'Edit report' page has three key buttons at the bottom.

The report can be submitted by clicking on the **'SAVE & STAY' (1)** button located under the content section. After clicking this button, the report form will be checked for errors. If no errors are detected, it will be submitted and saved in the database. If errors are detected, the user will be shown the section that contains the first error and the error will be marked in red.

Clicking on the **'BACK TO LIST' (2)** button will take the user back to the list of reports without saving the added information.

Clicking on the **'PREVIEW' (3)** button will take the user to the summary of this particular report without saving the added changes.



5.4. Users

Two main groups of users can access the platform:

- Anonymous users – are allowed to enter the front-end application and submit reports about incidents;
- Registered users – are allowed to enter the back-end application and manage reports.

The back-end application restricts access to functionalities through an authorization mechanism. To allow access to the back-end application, the IT administrator has to create an account for the user.

5.5. User Roles

To ensure the security of private data, the back-end application allows for creating users with different level of access. Each user has to be assigned to one of the following roles:

a. IT Administrator – This type of user has full access to all of the functions of the platform. The number of IT administrators should be as low as possible and IT administrators should only be used to create other users and perform actions that are restricted to other types of users.
b. Content Administrator – This type of user is allowed to modify the content of the front-end application and to assign new incidents to certain groups. They can also view and modify some of the sensitive data that is invisible to users with lesser privileges such as users and guests. In cases when the platform is shared by multiple organizations and thus has multiple groups, the content administrator is responsible for initially reviewing the reports and assigning them to groups to be managed.
c. Group Administrator – The main purpose of this role is to assign incidents to users, who are members of a particular group. Group administrators can also share incidents with other groups.
d. User – This is a general role designed to manage assigned incidents.
e. Guest – This is a type of user that is only allowed to view the incidents in a certain group, but is not allowed to edit any of the information stored on the platform.

The IT administrator can change user roles at any time, in case you need to ‘upgrade’ or ‘downgrade’ a user.

Tip. When assigning roles to different users, it is worth considering the following questions:

- Is the platform shared with other organizations or used by a single CSO?
- How many members of your staff will be using the platform regularly?
- What are the foreseen duties of each member of your staff when using the platform?
- For what purpose(s) will each user be using the platform?
- Who will be responsible for IT administration?
- Who will serve as the focal point within the organization and be using the platform most regularly?
- If the platform is used by a coalition of CSOs who will be your focal point for communicating with coalition partners?
- What kind of personal data will you be processing and who do you want to have access to it?

After considering these questions, organizations should assign users to the roles that will allow them to perform the assigned duties in the best possible manner. It might also be a good idea to map out the workflow in the organization or plan the tasks of each team member and assign user roles to them based on this plan.

Tip. Having different user roles can allow for better protection of sensitive private data and for smoother workflow in coalitions or larger organizations. However, not all user roles have to be filled. Small organizations, where only one individual is working with the platform, can use it through a combination of an IT administrator (for occasional fixes) and a content administrator (for data management).

Point of caution! Avoid sharing a single account between multiple people. User accounts and roles given to each user should correspond with the actual roles of individuals in their organization. It is advisable to avoid creating too many administrator accounts. Try to use the IT administrator account only for administration purposes. If one user has two roles in the organization it would be better to create two accounts for him or her instead of having a single account with higher privileges. Such cautionary measures will contribute to the security of sensitive private data stored on the platform.

Point of caution! People given temporary access to the platform should sign a confidentiality declaration confirming their compliance with your organization’s data protection policy.

5.6. Back-end Application Permission Matrix

The permission matrix below can help you decide which role should be given to which user and should help you plan the workflow.

Permission	IT Administrator	Content Administrator	Group Administrator	User	Guest
Dashboard					
Access own dashboard	x	x	x	x	x
Access dashboards of other users	x	x			
Reports					
View the list all incident reports	x	x			
View the list of incident reports assigned to their group	x	x	x	x	x
Create new reports	x	x	x	x	
Edit reports that are not yet assigned to a group	x	x			
Edit reports that are not yet assigned to a user	x	x	x	x	
Edit reports assigned to them or their group	x	x	x	x	
Delete reports	x	x	x		
Edit report summary	x	x	x		
Assign report to user	x	x			
Assign report to group	x	x	x		
Share reports with members of other groups	x	x	x		
Preview report summary	x	x	x	x	x
Print report summary	x	x	x	x	x
Preview report shared to their group	x	x	x	x	x
Print reports shared to their group	x	x	x	x	x
Export reports as .xls file	x	x	x	x	
Users					
View the list of users	x		x		
Create new users	x				
Edit existing users	x				
Delete users	x				
Remove users from groups	x		x		
Groups					
Assign users to groups	x				
View the list of groups	x	x			

Create groups	x				
Edit groups	x				
Delete groups	x				
Assign group administrators	x				
Settings					
Modify application settings	x	x			
Translations					
Modify translations	x	x			
Logs					
View and print activity logs	x	x	x	x	

5.7. User List

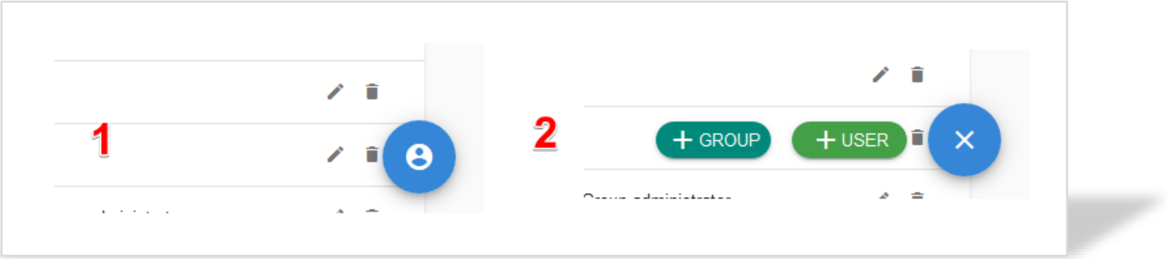
The list of registered users is available to view and edit only for the IT administrator. The list of users can be navigated and controlled in a similar way to the list of reports, and the users displayed on the list can be sorted based on values in different columns.

The user list has the following columns:

Name – This text is hyperlinked. Clicking on the user's name will lead to the individual dashboards of users, which contain the logs of user activities.
Email – This section contains simple text.
Groups – This text is hyperlinked. Clicking on the group name will take one to the list of reports assigned to that particular group.
Removal from group icon – Clicking on this icon allows the IT administrator or group administrator to remove the user from a given group.
Role – This section contains simple text.
Editing and deleting icons – Clicking on these icons will take the IT administrator to a special interface for changing user information and for deleting users.

5.8. Creating Users

To create a user, go to the user's list (Menu > Users), and click the blue button located in the bottom right-hand corner of the screen (1). It will expand into '+GROUP' and '+USER' buttons. To create a new user click '+USER' (2). This will prompt a user creation form.



User Form

To create a new user, the IT administrator will have to fill in the following information:

Name – This field should contain the full name of the user.
E-mail – This field should contain a unique e-mail address. The email address will also serve as a login.

Password – This is a text field. The password has to be at least 6 characters long, and must contain at least one capital letter and one number. The user will be able to change the password at any time after logging in through the ‘Profile’ section available at the top right corner of the page.
Password confirmation – This is a text field. The text in this field has to match the text used for the ‘Password’ field.
Role – This is a dropdown field. It asks for choosing the user’s role.
Groups – This is a multiple choice dropdown field. It allows assigning users to one or more groups. Note, that if a user’s role is ‘Group Administrator,’ assigning this user to a group will not make him or her the administrator of the selected groups.
Group management – This is a dropdown field. This field appears only when the user role is selected as ‘Group Administrator’. It allows setting which groups this particular user will administer. Alternatively, to give the group administrator the permission to manage a group, please go to the *Groups* section of the back-end application and see: *8. Settings. Groups* section of this manual.

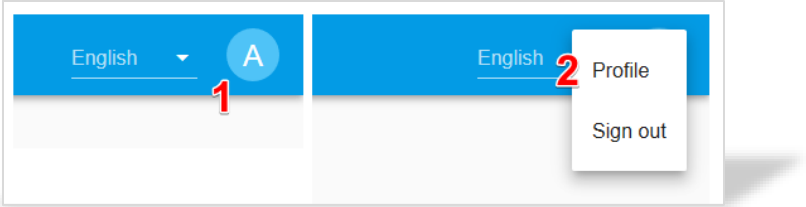
5.9. Editing Users

The information about users can be edited by:

- Users themselves;
- IT administrator.

Editing Your Personal User Profile

If users want to change their account information, they should (1) click on the user profile icon on the top right-hand corner of the header and (2) click on ‘Profile’.



This will take the user to their individual user profile form. Regular users can change their name and password. All other information can only be changed by the IT administrator.

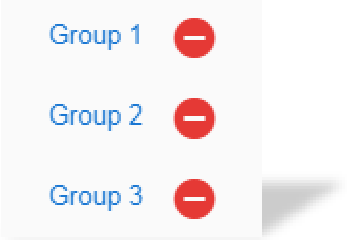
Editing User Profiles for IT Administrators

The IT administrator can edit profile information about all the users that have access to the back-end application. In order to edit profile information of other users the IT administrator should go to ‘Menu > Users’ and click on the pencil icon next to the user whose information they would like to edit. This will take the IT administrator to the profile page of the selected user, where they will be able to edit the user’s name, email address, password, role and group belonging. The IT administrator can edit any of the fields available. To save the changes, the IT administrator should click the ‘SAVE USER’ button. A notification will appear and the screen will automatically reload back to the main list of users.

5.10. Removing Users from Groups

Only IT administrators can assign users to groups. However, IT administrators, content administrators and group administrators have the power to remove users from the groups that they manage. This can be done through the main list of users.

The removal icon is displayed next to the group name that indicates users belonging to a particular group. Click on the red icon to remove a user from each of the groups. A pop-up box asking for confirmation will appear, click either ‘Unassign’ or ‘Cancel’. The IT administrator can remove any user from any group. However, group administrators can remove users only from the group that they are managing.



5.11. Deleting Users

Only IT administrators can delete users. To delete a user go to ‘Menu > Users’ and click on the rubbish bin icon next to the user you want to delete. A confirmation pop-up box will appear. Click either ‘Cancel’ or ’Delete’ based on the desired course of action.

6. Settings: General

6.1. Interface: General Settings

Default language – This is a drop down field. It sets the default language used in the front-end and back-end applications

6.2. Interface: Front-end Settings

This section allows IT administrators to choose the questions that will be displayed in the reporting form on the front-end application. To change the field visibility on the reporting form, switch the desired field on or off and click the ‘SAVE SETTINGS’ button on the bottom of the form. To edit the text of each of the questions as they are displayed, go to ‘Translations >’ which will allow editing the questions in all language versions of the application. For more information about translations see: *10. Translations.*

Point of caution! Generally, to comply with the General Data Protection Regulation (GDPR) the file upload question should be switched off if the reporting form is publicly available. The files uploaded by reporters may reveal sensitive private information about third parties whose consent data has not been obtained.

7. Settings: Groups

The platform can be used by a single CSO or a coalition of CSOs that agree to share the back-end database and the reporting form. In cases where the platform is used by a single CSO, all users (regardless of their role) will be assigned to a single group. If the platform is used by several partnering CSOs, platform users can be grouped according to the CSOs they belong to.

Dividing users into groups based on their organization allows for better management of private data and ensures that each coalition partner has ownership and control of the information that they receive and manage.

Each user (regardless of their role) can be assigned to one or more groups. Members of a group can all see the reports that are assigned to that particular group. If groups want to share their incident reports with other groups or specific users, this can be done by either (1) sharing individual reports with other groups (see section 5.2) or (2) adding users to a specific group (see section 6.4). Group management functions are only available to IT administrators.

7.1. Group List

All groups created on the platform will be displayed on the group list, found at 'Menu -> Settings -> Groups'. The list displays group names and their administrators. To change the group's name or administrator, click on the pencil icon. To delete the group, click on the rubbish bin icon.

7.2. Creating Groups

There are two ways to create a new group:

1 – Go to 'Menu -> Users' and click on the blue button in the bottom right-hand corner and then choose 'Group.'

2 - Go to 'Settings -> Groups' and click on '+' button in bottom right-hand corner of screen.

Both of these options will take you to a simple form for adding new groups.

Group Creation Form

This section consists of two questions:

Name – This is a text field for inserting the group's name.

Administrator – This is a drop down list. Chose a user from the list to administer the group. Only users that have the role of a 'group administrator' will appear on the drop down list.

Click 'Add group'.

7.3. Adding and Removing Users from Groups

Users can be added to or removed from groups through the 'Menu -> Users' section.

To add a user to a group, go to 'Menu -> Users' and click on the pencil icon next to the user, which you want to add to any of the groups. On the 'Edit User' page, under the 'Group' question, tick the box next to the names of groups to which you want to add the user. Press 'Save user'.

There are two ways of removing users from groups:

1– For IT administrators, use the same path as for adding users to a group, but simply untick the relevant boxes.

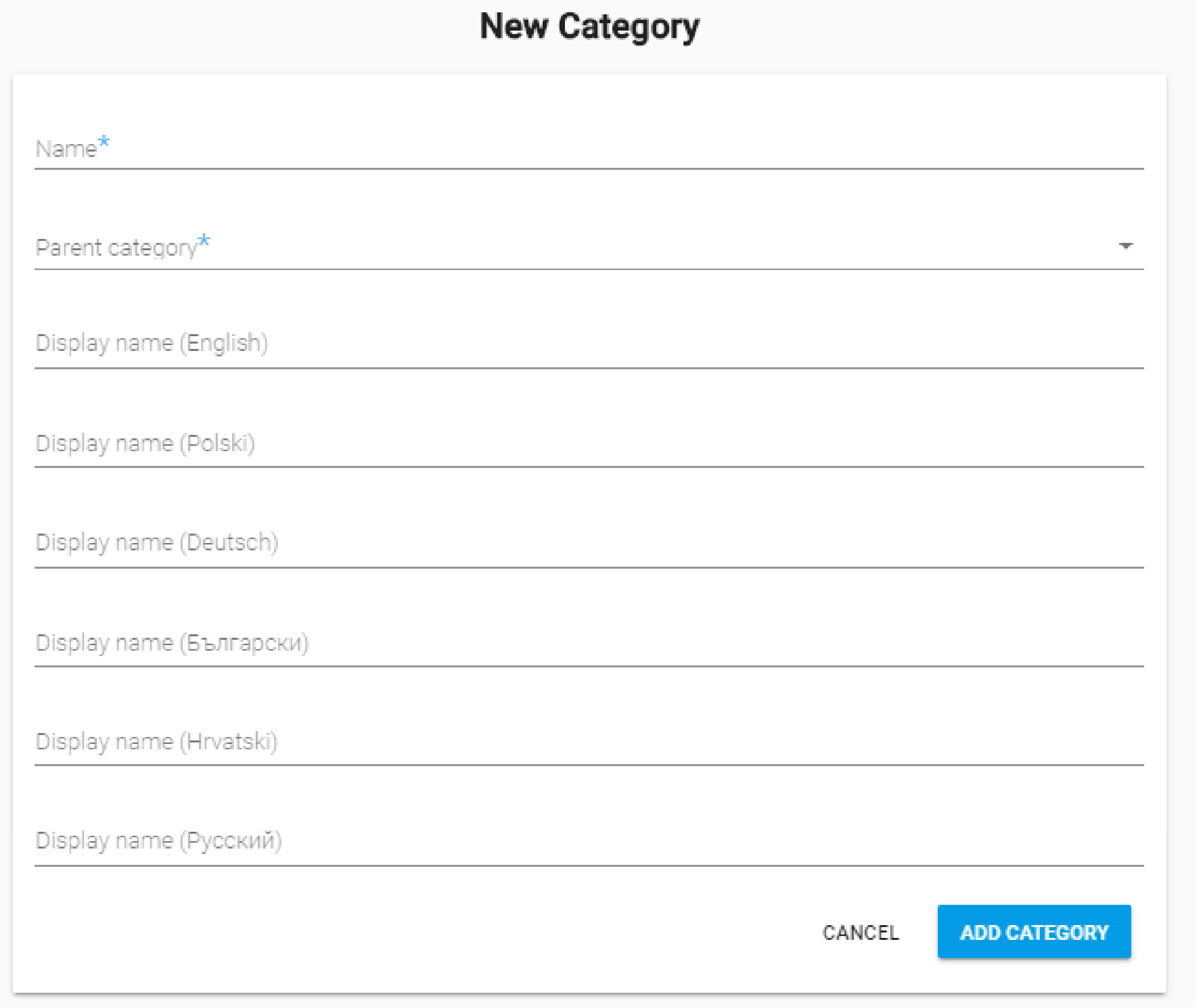
2– For group administrators, go to 'Menu -> Users', click on the red icon next to the group name in the row of the user in question.

8. Settings

This part allows administrators to create the incident classification categories that later will be used to classify different incidents. The list of classification categories have the same navigation elements (editing, deleting, sorting) as the lists of users and groups.

To create a category click on the blue '+' sign in the bottom right corner of the screen. A new window will appear. In that form you should enter the name of the incident category, select its 'parent category' (if you are creating a sub-category of an already existing one). To save the information you entered, click on the 'Add category' button. To see the new changes reload the page.

The default categories available in the platform follow ODIHR's hate crime monitoring methodology and additionally include hate speech and discrimination.



Point of caution! Major edits to the 'tree' of classification categories should be done before starting to use the platform actively, as adding and especially deleting categories when the database already contains reports can confuse the flow of information in the platform.

9. Translations

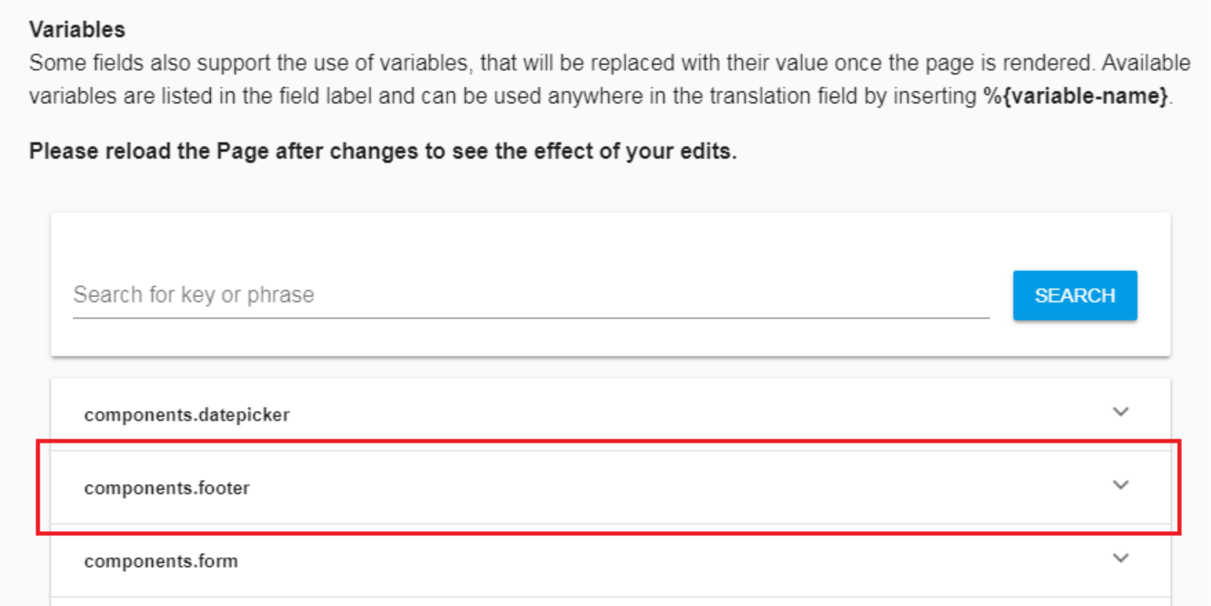
Both back-end and front-end applications are fully translatable. The number of languages in which the platform will be available can be chosen during the installation process. Users with IT administrator and content administrator roles are allowed to change translations. Through the translations section IT and content administrators can also change and edit the original English text displayed in the platform. Translations are divided into four main groups:

- **Common** – This section includes pieces of text that appear in the platform multiple times in different sections. It mostly contains various error messages, general pop-ups and bias motivations used for analyzing the incidents.
- **Front-end** – This section contains bits of text displayed on the front-end application. This section allows for changing any of the text displayed on the front-end application and for adjusting the formatting. The text of questions in the reporting form can also be changed here.
- **Admin User Interface** – This is the largest translation section, which includes most of the pieces of text displayed in the back-end application.

- **Emails** – This section allows setting up and translating the text of automatically generated emails that will be delivered to the administrator and the reporter after an incident is received through the reporting form.

9.1. Translation Form

To translate a phrase, select the main translation group from the side menu and then search for the necessary phrase on the list. Phrases inside the selected main translation group are also grouped into smaller groups to make browsing easier.

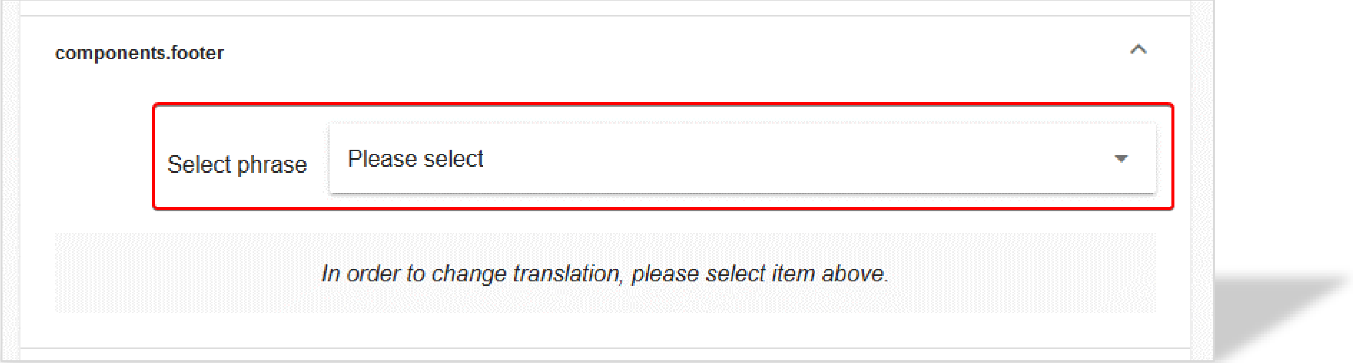


Variables

Some fields also support the use of variables, that will be replaced with their value once the page is rendered. Available variables are listed in the field label and can be used anywhere in the translation field by inserting **%{variable-name}**.

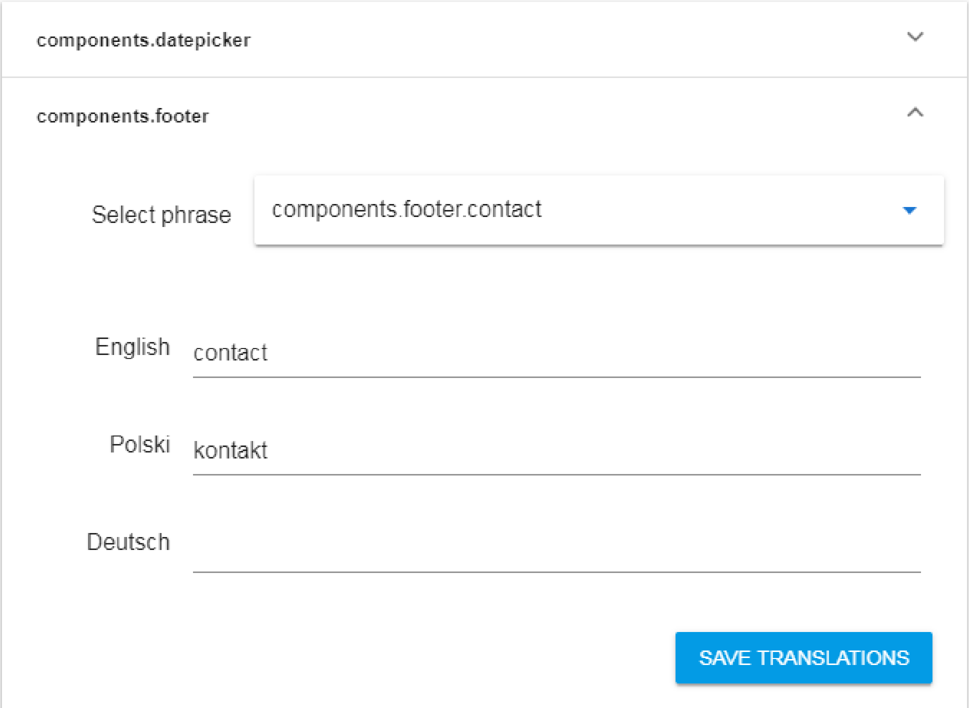
Please reload the Page after changes to see the effect of your edits.

After selecting grouped translation phrases, you will be able to choose the phrase that you wish to translate:



In order to change translation, please select item above.

After choosing the phrase, the translation form will open and the user will be able to translate the phrase into any of the languages of the application.



components.datepicker

components.footer

Select phrase: components.footer.contact

English: contact

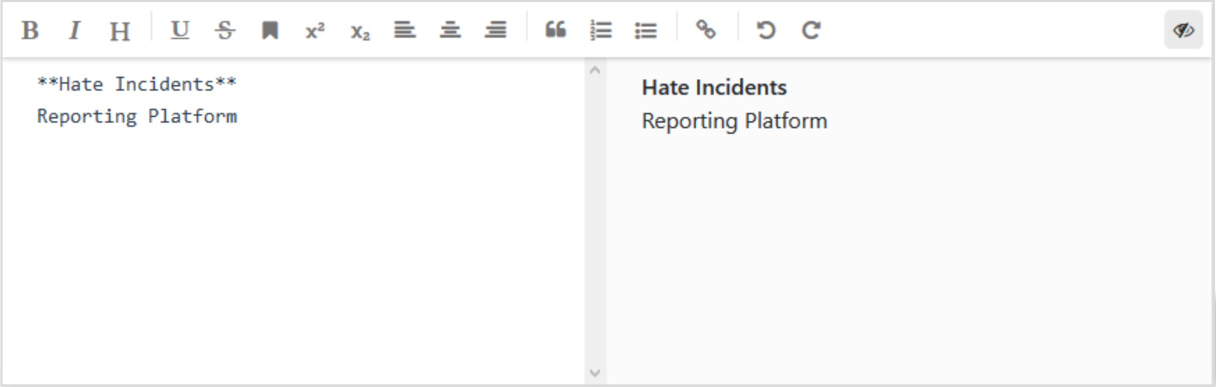
Polski: kontakt

Deutsch:

Tip. The translation search applies to both the hardcoded names of fields, and the actual text of the translations. It is possible to search for a specific word in a specific language.

9.2. Markdown Format

For some translations like headers or page contents, it is possible to change the formatting using the Markdown Editor.



```
**Hate Incidents**
Reporting Platform
```

Hate Incidents
Reporting Platform

Markdown is a lightweight markup language that you can use to add formatting elements to plain text documents. For instance, to denote a heading, you add a hash sign before it (e.g., # Heading One) or to make a phrase bold, you add two asterisks before and after it (e.g., **this text is bold**).

The Markdown Editor with two parallel screens allows editing the elements of the text and seeing how they will be displayed on the application.

Basic Syntax

Element	Markdown
Heading	# First level heading ## Second level heading ### Third level heading
Bold	**bold text**
Italic	*italicized text*
Blockquote	>
Ordered List	1. First Item 2. Second Item 3. Third Item
Unordered list	* First Item * Second Item * Third item
Code	`code`
Horizontal Rule	---
Link	[title](http://somewebsite.com)
Image	![alt text](https://link.com/example.png)

For more information about Markdown Syntax visit https://www.markdownguide.org/cheat-sheet

Point of caution! If you are operating the platform in several languages, make sure that implemented edits match the text and formatting in corresponding sections.

Tip. Depending on the target audience and capacities of the staff operating the platform, the front-end can operate in multiple languages and the back-end in only one or vice versa.

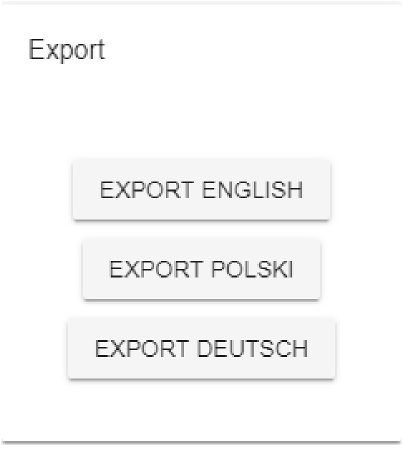
9.3. Uploading or Downloading Translations

The platform allows to upload or download all text available in a single language at once as a single YAML (.yml) file. This option may be useful if you would like to introduce a new language into the platform and want to translate the entirety of the interface at once or would like to send it to a translator.

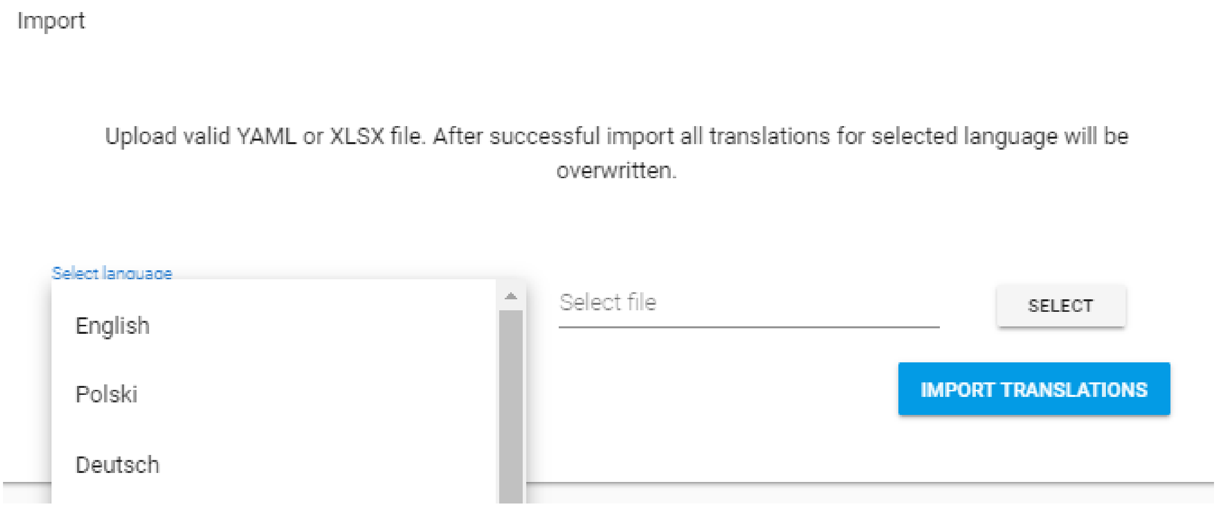
The files can be exported or imported in YAML format. YAML uses a text file and organizes it into a format which is human-readable. YAML files can be opened using basic text readers such as notepad or notepad++. YAML files can be conveniently edited using free software, such as 'Visual Studio Code'.[8] They can also be easily converted to more popular .csv or .xlsx formats.

[8] https://code.visualstudio.com/

To download the existing translations go to ‘Translations -> Import/Export’. On the upper left-hand side of the page a list of all available translations will be displayed. Click on the specific translation that you would like to export.



To import new or updated translations, go to ‘Translations -> Import/Export’ and use the upper right-hand side of the page. Select the language of the translation you are about to upload, select the relevant file form your computer and click ‘Import translations’.

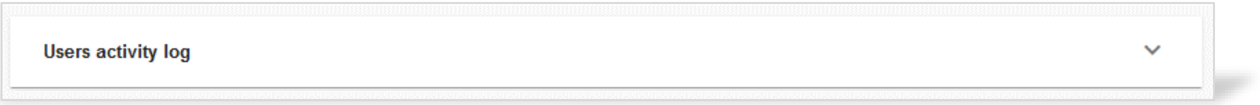


Upload valid YAML or XLSX file. After successful import all translations for selected language will be overwritten.

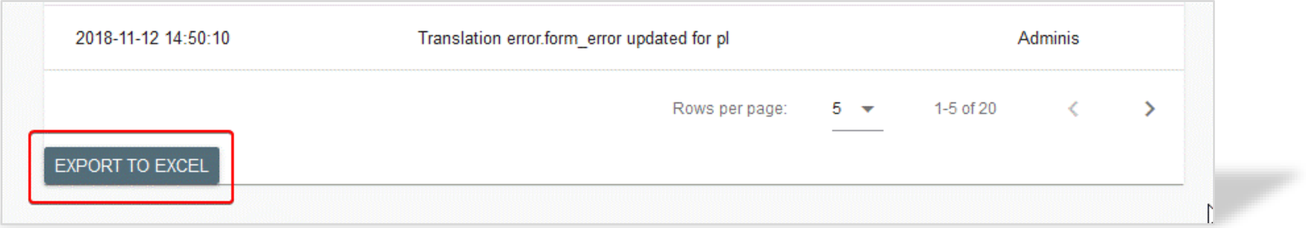
10. Logs

To improve the platform security and keep track of changes made in the application, a logging mechanism registers each action taken by the users. Usually logs are displayed on the bottom of the screen as a simple table containing recent actions related to the current part of application.

To preview logs, click on ‘Users activity log’ bar placed at the bottom of the screen.



Users can export logs to Excel by clicking on the ‘EXPORT TO EXCEL’ button placed in the bottom left-hand corner of each log table.



2018-11-12 14:50:10 Translation error.form_error updated for pl Adminis

The log exported to Excel contains the following information:

- Time of action
- IP address of user who performed the action
- Action
- User ID
- Entity ID
- Entity type
- User agent
- Raw data

Application Pages that Contain Users’ Activity Logs:

- User's dashboard – logs all main actions by the user whose dashboard is displayed.
- Report summary – logs all actions any of the users performed with the report displayed.
- Users -> Edit User – logs all changes to the given user profile.
- Settings -> Interface – logs all changes to the interface settings.
- Settings -> Groups – logs all changes to the group information.
- Settings -> Categories – logs all changes to the classification categories.
- Translations – logs all translation changes.