



RESIST

Fostering Queer Feminist Intersectional Resistances against Transnational Anti-Gender Politics

RESIST Privacy Policy

Who are we?

This privacy policy is for the RESIST research project, which has now ended. This project is no longer collecting any data; details of data stored after the project end (September 2026) are included in this policy. It also retains the details of the terms under which the data was collected. In 2036, all data will be destroyed unless consent has been given to archive it.

During its lifetime, RESIST fully respects your right to privacy and actively seeks to preserve the privacy rights of those who share information with RESIST. Any personal information which was volunteered to RESIST is treated in accordance with European Data Protection legislation.

Why and how do we collect and process the information?

We collected your personal data on the bases of:

1. Consent, where the individual has given clear consent for us to process their personal data for this specific purpose as stated in the participant information.
2. The project fulfilling a public task that has a clear basis in law. The processing is necessary for us to perform a task in the public interest or for our official function bestowed upon us by the State.

We collected the following types of personal data:

What:

Personal Data

- First name & surname
- Contact details (email address and phone numbers)
- Consent forms with name and signature
- Demographic data (not kept with other personal data, only associated with a participant's name and research data if requested)

Research Data

- Interview/focus group/workshop audio files, transcripts and findings summaries
- Organisation materials and tactics
- De-identified comments made under the public facing project social media.
- Online questionnaire responses
- Relief maps

How:



UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG



Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN



Funded by
the European Union

WP2: In-depth interviews, focus groups, relief mapping and a short questionnaire across 9 case studies.

WP3: Expert interviews with CSO representatives and workshops with feminist organisations across 10 case studies.

WP4: Online workshops with WP3 participants and other expert consultants from 10 case studies.

Purpose:

- Contact details of participants and expert consultants are stored to arrange interviews/focus groups/workshops.
- Contact details of organisations, media actors and public figures are stored to send key information to stakeholders.
- Research data was collected to fulfil the purpose of the research.

How long will we store your data?

Raw research data will be destroyed 10 years post-project (2036), and will not have been submitted to a repository in line with the UCD Research Data Management Policy https://hub.ucd.ie/ucis/!W_HU_MENU.P_PUBLISH?p_tag=GD-DOCLAND&ID=227.

De-identified research data stored on Zenodo is retained for the lifetime of the repository, which is based on the lifetime of the host laboratory CERN, which currently has an experimental programme defined for the next 20 years at least. In the case of the repository closure, efforts are made by Zenodo to integrate content into a suitable alternative repository. The metadata of the original data object/data, including the DOI, is retained by Zenodo even if the data is withdrawn.

Personal data for WP2 participants and WP3 interview participants was kept until the time of analysis and then only with participant consent, and kept locally and in UCD. After this it was deleted, unless the participant consented for their name to be used alongside their research data or for their contact details to be stored for communications regarding project updates. Personal data for CSOs is kept at least until the end of the project for communication regarding WP4 workshops, their previous workshop contributions, and events such as the final project conference. CSOs can withdraw their contact details by notifying the researcher they are in contact with.

Personal data for WP4 expert consultants is kept by the WP4 lead researcher until the end of the project for communication regarding the WP4 outputs. They can withdraw from the process by notifying the WP4 lead researcher.

WP2 & WP3 participants were offered fully informed, opt-in consent and the right of withdrawal. Participants had to opt in to the archiving of data and had the right to withdraw their data from interviews, focus groups, group discussions and findings summaries until the time of analysis. After this point the findings summaries were incorporated into the analysis and could not be separated out. In addition, the use of English means that applying directly to UCD to withdraw data was not feasible given the variety of languages in use. This withdrawal process also ensured that GDPR-wise we only keep personal data for the time that it is required for withdrawal and thereafter on an opt-in basis. The process for withdrawal was:

1. Participants could contact the local researcher/case study lead whose details are on the information sheet and consent form to say that they wished to withdraw their data. They would use the same contact details that they have communicated with the project (e.g. same email address/phone number).
2. This information would be used to relink interview/focus group data with participants locally (i.e. not through UCD). For this purpose a key linking participant IDs with personal details was kept securely and separately locally. It was backed up locally to avoid loss of data.
3. The local files (audio recordings/transcripts/findings summaries - interviews, direct quotes from findings summaries for focus groups) would be deleted. In the case of a focus group, participant direct quotes would be deleted.
4. UCD would be informed of the participant identification for interviews and materials deleted. New focus group summaries would be sent and would override those stored at UCD.

We kept personal data until analysis, and only with consent. This was kept locally and in UCD. Contact data was deleted at the point of analysis, unless the participant has consented for their name to be used alongside their research data or for their contact details to be stored for communications regarding project updates.

Participants gave permission to store their personal data up until the point of analysis in order to be able to withdraw their participation if requested. Withdrawing research data was only possible within the terms of the research - once the findings were public it was not possible to alter or withdraw data, as this undermines data quality checking which requires going back to raw data at times to validate the findings.

Participants had an opportunity to check the findings summary to confirm it was accurate. This was not given to focus group participants as these were collective summaries not individual responses. This was an opt-in where participants could request that the findings summary was sent to contact details provided. For interview findings summaries in the Belarus case study, where an electronic means is not possible, participants could opt-in for the researcher to read them the interview findings summary and seek a verbal agreement.

Participants had to opt in to the archiving of their research findings summary. All focus group participants had to consent to the findings summary being archived in order to take part but could opt in to their specific stories being recorded.

Who has access to the information and who we share it with?

Organisations with legal responsibility for the processing of your personal data: The personal data collected is accessed by project partners at Edinburgh Napier University; European University Viadrina; Feminist Autonomous Centre for Research; Hochschule Luzern; National University of Ireland Maynooth; University College Dublin; Université de Fribourg; Université de Lausanne; Universitat Pompeu Fabra; Paris 1 Panthéon-Sorbonne.

Third-Party service providers the project uses to process your data based the project's instructions: RESIST shared data with third parties where necessary for purposes of the processing outlined The University shared personal data with these EU GDPR compliant parties:

- Airtable - to securely store data
- Transcription tools - to transcribe recorded interview or focus group audio
- Google Drive - to securely store data
- Online questionnaire tool to gather questionnaire responses
- Newsletter tool for those who choose to sign up for project updates

The personal data is accessible in Switzerland under the GDPR Article 45 international transfer mechanism (transfers on the basis of an adequacy decision).

Storage drives are segregated to only allow researchers access to the areas that are required for processing their data and accessing data that is needed to meet the objectives of the action. University-managed data storage is resilient, and is protected against corruption through digital off-site back-ups.

There is restricted access to raw data by researchers. Data stored on the data server is automatically backed up regularly to a sister backup server, also only accessible via VPN, and only by maintenance and support.

Personal data is processed in compliance with, and benefits from, the protection of European privacy legislation. This includes server locations used.

For more information about participating in RESIST, please see our information sheet.

Relief Maps: This component of the project did not collect or process any personal data. The sensitive data collected from this study (never linked to personal data) was encrypted as quickly as possible after data collection and prior to being stored on the database to prevent the re-identification of each data subject. All participants were de-identified and allocated a coded participant ID # for the duration of the study. The website is hosted at the UPF server.

GDPR compliant cloud-based transcription software was used to aid the creation of WP2 and WP3 data findings summaries if the case study lead decided it was appropriate. The recordings were only located on the cloud for as long as required to process the data - after which point they were deleted from the transcription site.

What are your rights?

The right to access – the right to request RESIST for copies of your personal data.

The right to rectification – the right to request that RESIST correct any information you believe is inaccurate, and the right to request RESIST to complete the information you believe is incomplete, until the point of analysis.

The right to erasure – the right to request that RESIST erase your personal data, under certain conditions.

The right to restrict processing – the right to request that RESIST restrict the processing of your personal data, under certain conditions.

The right to object to processing – the right to object to RESIST processing of your personal data, under certain conditions.

The right to data portability – the right to request that RESIST transfer the data that we have collected to another organisation, or directly to you, under certain conditions.

The right to withdraw consent

If you make a request, we have one month to respond to you. If you would like to exercise any of these rights, please contact us at kath.browne@ucd.ie.

If you have concerns about your rights as a participant, you can contact the DPO at your researcher's institution.

- UCD Data Protection Officer: Data Protection Officer, Roebuck Castle, Belfield, Dublin 4, Ireland. Email: gdpr@ucd.ie
- ENU Data Protection Officer: Email dataprotection@napier.ac.uk
- EUV Data Protection Officer: Data Protection Officer, Große Scharrnstr. 59, 15230 Frankfurt (Oder), Germany. Email: datenschutz@europa-uni.de
- FAC Data Protection Officer: Myrto Tsilimpounidi. Email: myrto@feministresearch.org
- HSLU Data Protection Officer: Ruben Antenen, Lucerne University of Applied Sciences and Arts, Werftstrasse 1, CH - 6002 Lucerne. Email: ruben.antenen@hslu.ch
- NUIM Data Protection Officer: Cecily Giles, Rye Hall Extension, North Campus, Maynooth University. Email: dataprotection@mu.ie
- UniFR Data Protection Officer: Email dpo@unifr.ch
- UNIL Data Protection Officer: Mikhaël Salamin, Affaires Générales, Bâtiment Unicentre, UNC-317. Email: Mikhael.Salaminprivacy@unil.ch
- UP1 Data Protection Officer: Email dpo@univ-paris1.fr
- UPF Data Protection Officer: Marc Vives Pizá, Universitat Pompeu Fabra, Mercè Building, Carrer de la Mercè 12, 08002 Barcelona. Email: dpd@upf.edu

If you are not satisfied with UCD's response or believe we are not processing your personal data in accordance with the law, you can complain to the Irish Data Protection Commission. For more detail see: <https://www.dataprotection.ie/>

Changes to our privacy policy

RESIST kept its privacy policy under regular review and placed any updates on this web page. This privacy policy was last updated on 15 July 2026.