GALE THE GLOBAL ALLIANCE FOR LGBT EDUCATION

Data Protection Policy

Introduction

In May 2018, the European General Data Protection Regulation (GDPR) comes into force. The GDPR obliges organizations to protect personal data, makes it mandatory to allow contacts to see and edit or delete their data. This policy makes transparent which data are collected by GALE and which measures are taken to protect the data and how we manage them, and how we manage risks.

Legally, GALE is a foundation based in the Netherlands. The foundation maintains a website which functions as a platform for an informal association. This means the GALE Foundation is legally responsible for the data on the platform.

GALE aims to enhance the quality of education about sexual diversity and promote cooperation in this area. This implies we work a lot with lesbian, gay, bisexual and transgender people, with people with an intersex condition, and other people who don't conform to the traditional view of sexual and gender norms. We do this worldwide. In a range of countries, sexual diversity is taboo, forbidden or even legally labelled "terrorism". This makes the position of the members very vulnerable and data protection is an essential part of our work.

GALE already had data protection measures in place from the very beginning of the website platform in 2007. Although we do collect information about sexual orientation and gender identity for use in our membership management, choosing to be open about this has always been optional. In addition, we have always allowed and even encouraged vulnerable members to register as a GALE member with an alibi and non-traceable email address. But it does happen that people register at a young age and in a progressive country, and later decide to work in a country where homosexuality is illegal. Or they live in a country which is taken over by a fascist government and suddenly need to review or delete all their vulnerable data. Despite the measures taken, this may lead to risks that are potentially deadly. In this Data Protection Policy, we try to manage these risks in the full awareness that reducing the risk to zero is virtually impossible in this globalized and digital world. But where we can, we will take own measures and make members and partners aware of the risks and measures they can take themselves.

Date of publication: August 2019, 2018; second edition

Data Protection Officer and Register

The GALE Foundation has few staff. The director, Peter Dankmeijer, functions as the Data Protection Officer. He can be reached at p.dankmeijer@gale.info; +31 20 737 2959.
All data changed on the request of persons or shared will be noted in the GALE Data Register. The register will be available on request for the proper authorities.
GALE is based in the Netherlands and the Dutch Personal Data Authority (Autoriteit Persoonsgegevens) is the supervising authority.

Principles

The GALE data Protection Policy follows the rules of the European General Data Protection Regulation (GDPR). More specifically:

1. All our staff, volunteers, members and partners will be made aware of the risks of disseminating personal data and how to manage such risks.
2. We do not collect personal information which is not necessary for our functioning.
3. We ask persons permission to use their data for specific purposes.
4. Persons have the right to have their data edited or deleted.
5. When new products which involve personal data are developed, data protection will be part of the design process.

Impact assessment

GALE maintains the following databases and data. In the matrix we also indicate the location of the database, whether specific databases are editable by the contacts and our risk assessment.

Impact assessment matrix

databases	objective	storage	access	risk level
ONLINE				
GALE members	membership policy and exchange	gale.info	moderators	high
Linked to profiles:				
Internal listserve	interactive communication between members	gale.info	moderators	low
Internal maillists	informing members	gale.info	moderators	low
Stand alone:				
Internal listserve	interactive communication between non-members	gale.info	moderators	low
Internal maillists	informing non-members	gale.info	moderators	low

Date of publication: August 2019, 2018; second edition

Moodle users	enabling participation in courses	sexualdiversityacademy.org	moderators	low
Oher processors				
Tentoo	salary payments	https://tentoo.nmbrs.nl	director	low
PFZW	pension payments	https://www.pfzw.nl	director	low
Consense	monitoring sick leave	https://www2.humannetverzuim.nl	director	low
CLOUD				
Central directory	contact management	tresor	dir/secr	low
Project databases	contact management	tresor	staff	low
Project logs	process management	tresor	staff	low
Research databases	collecting statistics	google sheets	staff	low
OFFLINE				
Outlook	contact management	hard drive	dir/secr	low
Cell phones	contact management	synced	staff	low

General risks

We have divided the risks on three levels: high, medium and low. High risk refers to serious risks for GALE members if their profile would be leaked. Medium risk refers to consequences of other databases that could be leaked. These don't contain data about sexual preference or sexual orientation and their location is secure. Low risk refers to online data that is securely processed and Cloud and offline data that is securely storage.

GALE member profiles

Due to the vulnerability of the LGBTI target groups, we assess the GALE members profiles as high risk (see paragraph specific risks). Internal listservs (interactive mailing lists) and internal mail lists are connected to the profiles on the website, but since these are only visible to members who want this and for moderators; therefore, we assess the mail lists themselves as a low risk.

Non-public databases

The central contact management database of GALE, temporary project address databases and temporary project logs containing names are in an encrypted Tresor Drive of the director. Tresor has been chosen for a limited Cloud service because it's encryption does not allow outsiders or governments to access the files in any way. The provider and servers are in Switzerland, which reduces the risk of other governments like the USA sharing these data with other governments. Only the director and his secretary have access to this PC and the Tresor Drive. This is considered low risk. These databases do not contain information that can be damaging when they are leaked.

GALE regularly does small scale research. For this, Google Forms and Google Sheets are

used. The research data are usually anonymous. In specific cases, names may be asked when data represent personal suggestions that need to be traced. These data are considered low risk.

Personal contact databases

The personal (and partly professional) contacts of the director and staff are stored in the Outlook profile of the director and personal address books of staff. The Outlook address book of the director is synchronized between the PC, laptop and phone. These are considered low risk because only loss of theft poses a risk.

Specific risk: GALE member profiles

The main risk is the database of members profiles on the website platform. The database is meant to support exchange between members and contains a lot of fields to enable such exchange and cooperation:

- First and family name
- Gender and sexual orientation
- Public summary of the profile
- Country
- Postal address
- Phone
- Email
- Password (hidden)
- Photo
- Areas of interest
- Areas of experience
- Looking for
- Available for
- Visibility of profile
- Declaration of agreement with the alliance guidelines

The fields on sexual orientation and gender identity are also used by the foundation to manage the recruitment and volunteer policy: the aim is to maintain a balance between LGBTI and heterosexual members and to maintain a gender equity. The country field is also used to develop policy to maintain an equitable North-South balance in the membership. There is a great concern that members from progressive and further developed Northern countries become too dominant and will define the cultural and strategic interaction within the association. However, such information, while necessary, also poses risks.

Date of publication: August 2019, 2018; second edition

Although potential members are informed about potential risks, it does happen (infrequently) that members are at risk because of their profile. Instances that happened in the history of GALE are:

- A member is from a country where sexual diversity is taboo and illegal, but when registering, there was not active persecution and access to internet was low in the country at the time. Five years later, the government and Muslim vigilante groups start active persecution of people who are critical of the government and/or of Islam. Identifying as LGBT or promoting equal opportunities or dialogue is deemed to be "terrorism against the State and the national identity" (a radical version of Islam). The GALE member is at acute risk because of death threats and the GALE profile is used as "evidence". GALE deletes the profile, but the page remains in the Google cache. Only the GALE member can submit a request to Google to remove the page from the Google cache; this can take a few weeks. Although the GALE profiles themselves are protected against Google search, when a member open a profile, Google may pick up this traffic from the browser and store it in their cache. GALE can only warn members against this but has no influence over the web browsing of members nor over the Google policy.
- A member from a progressive Northern State is going to work as a researcher on human rights in a State where Islam is dominant and where the LGBT movement is increasingly targeted by vigilante Muslim groups. The State has adopted a law which says that discussing sexual diversity online equals porn and is a punishable threat to family life. The member wants his profile to be deleted or to be altered with a pseudonym. The profile is edited with a pseudonym name and different email.
- A member from a State where Hinduism is dominant and where the radical Hindutva movement starts persecuting non-Hindus and "non-pure" citizens, fears that his opportunities for a job will be hampered by his GALE profile and wants to remove it. The profile is removed.

These examples show that the risk is often related to changing circumstances in the private situation of the GALE member or in deteriorating contexts where they life or work. These changing situations can often not be foreseen. Apart from being cautious, transparent and flexible with the member profiles, creating awareness of this to current and future GALE members is important.

Measures

GALE distinguishes between general measures and specific measures. The general

Date of publication: August 2019, 2018; second edition

measures are valid for all circumstances. The specific measures are relevant for specific databases or events and deal with the management of specific risks associated with these databases.

General measures

Websites

1. The website www.gale.info is protected with a https certificate and the web host YPOS has integrated GDPR compliance in the website system. The website system is automatically regularly upgraded by YPOS to maintain the highest standards. Passwords used for the site are encrypted and transfer of data online is SSL encrypted. These protections are formally agreed upon in a Processor Agreement between GALE and YPOS.
2. The Moodle website www.sexualdiversityacadmy.org is protected with a https certificate and the web host Avetica has integrated GDPR compliance in the website system. The website system is automatically regularly upgraded by Avetica to maintain the highest standards. Passwords used for the site are encrypted and transfer of data online is SSL encrypted. These protections are formally agreed upon in a Processor Agreement between GALE and Avetica.
3. When we ask for personal data, we indicate the purpose and ask permission to maintain the data and inform how the person can edit or remove the data.
4. In case of a (perceived or real) data leak, the staff, volunteer, member or data processor immediately informs the Data Controller who will order or take appropriate measures.
5. The online profiles in the GALE website and in Moodle are submitted by users and can be edited and removed by them. Once every five years, profiles that are not used (Moodle) or that have incorrect data (non-accessible email addresses) are removed.
6. Temporary listservs or mail lists (for projects or specific tasks) are deleted after completion of the tasks.
7. Permanent listservs or mail lists are kept indefinitely, but the members are informed how they can edit their data of have their data removed.

Research

Normally, GALE research is anonymous, and the data cannot be traced to individuals. In some cases, such a link is necessary, for example when doing a qualitative needs assessment among a small but expert target group. In those cases, respondents will be

informed of the goal and about the use of their data. After online collection, the online database will be deleted, and the data will be offline stored in a secure location.

PC, laptop and phone protection

PC's, laptops and phones of staff are protected with passwords and/or fingerprint access and protected against viruses and ransomware with Bitdefender.

Portable data carriers

GDRP sensitive files on USBs and data backup drives will be encrypted and only accessible with passwords.

Data Leak Procedure

When data leaks occur or may occur, a Data Leak Memo will be filed which contains:

1. Date, time and place of (possible) data leak
2. Date and time of discovery
3. Data and time of blocking access to the data
4. Probable cause
5. Measures taken to recover the item, erase or move the data
6. Correction measures to restore current protection and if necessary improve the design of the protection
7. Assessment of need to report to the Dutch Personal Data Authority (Autoriteit Persoonsgegevens) and decision
8. The memo is documented in the Data Register

Loss or theft of laptops, or phones or other data storage devices like USB's

When data are lost or stolen, the lost items will be blocked from use as soon as the loss has been discovered. The Data Leak Procedure will be followed.

Data portability

Data are kept or can be downloaded in MS Excel format. On request, persons can get copies of files with their data in this format. MS Excel files with personal data are not shared with third parties unless explicitly mentioned when registering. Change of data or transfer on the request of the person or transfer of data by GALE staff is documented in the Data Register.

Complaints

Persons can file a complaint about non-compliance with this Data Protection Policy or about the Data Protection Policy itself. The normal procedure for this is to write to the executive

director, who will deal with the complaint as soon as possible. In addition the GALE Complaint Procedure is applicable. Complaints are registered in the Data Register. Persons call also file a complaint at the Dutch Personal Data Authority (Autoriteit Persoonsgegevens).

Specific measures: members profiles

The online database of GALE poses specific risks. Apart from the mentioned general protections, GALE takes a series of additional measures to limit these risks:

1. In the instruction on how to make a profile, potential members are made aware of the risk now and in the future. They are also advised to register with a pseudonym if they think registering with a real name will put them at risk.
2. The profiles have four levels of settings of the visibility: 1. public, 2. for all members, 3. for members of groups the member participates in, and 4. only for moderators.
3. Except for the name and email, all profile fields are optional.
4. The fields about sexual orientation and gender identity contain multiple options including: “I do not identify with these categories”.
5. When a new member registers, the staff checks the profile and contacts the new member to welcome them. If the profile looks suspicious, the staff attempts to check the sincerity of the member. When there is no or an inadequate response, the new member profile is deleted by the moderator. In practice this usually happens with members who have only commercial interests or dating interests.
6. Incidentally, the GALE members database will be downloaded as Excel to prepare statistics necessary for the annual report of for policy reasons. Such a database will be only kept in archive with the personal data deleted or made untraceable to the involved persons.
7. When a data leak occurs of GALE members profiles, the Dutch Personal Data Authority (Autoriteit Persoonsgegevens) must be informed.

Guidelines for staff

All staff and volunteers will be made aware of the Data Protection Policy and guidelines when they start working for the GALE Foundation, or when they become member of the GALE web platform. It will especially be stressed how important privacy is for vulnerable GALE members.

Date of publication: August 2019, 2018; second edition

It will be expressly forbidden for staff to share personal data of GALE members through leaky Cloud services like Dropbox, Google Drive and OneDrive.
The staff will be made aware that any data leaks should be reported immediately to the director and that a Data Leak Memo needs to be filed to properly asses the risk and to be transparent about decisions and measures taken.

Review and storage

The Data Protection Policy will be reviewed every five years, or more often if incidents point to the necessity to update it.
During the review, datasets will be deleted or confirmed to remain active as part of ongoing used datasets.
Data collected in the context of projects will be deleted after the mandatory legal archive periods.

Information to the public

The Data Protection Policy is available on https://www.gale.info/en/foundation/accountability.
It will also be referred to on the information page for potential members.

Date of publication: August 2019, 2018; second edition