KERIC, NGO

Nábrežná 1351, Čadca 02201
Phone: +421 908 913 995
keric@keric.sk

KERIC DATA PROTECTION POLICY

INTRODUCTION

KERIC is a non-profit non-governmental organization working mainly with children and youth aged 7-30 as well as adults for last 16 years. We offer a wide range of activities with an extra added international dimension which develop the personality of children and youth and differ based on the needs of participants. Our mission is to connect as our region Kysuce as the rest of Slovakia with the whole world. To be able to full fill our mission KERIC needs to gather and use certain information.

This information can be about people who come for activities organized by KERIC, employees, volunteers, partners from other organizations, local partners, family members and all the other people we have relationship with and may have be in contact with.

This policy describes how this personal data must be collected, handled and stored to meet the organization's data protection standards and to comply with the law.

WHY THIS POLICY EXISTS

This Data protection policy ensures KERIC:

- Complies with data protection law and follow good practice
- Protects the rights of people who come for activities organized by KERIC, employees, volunteers, partners from other organizations, local partners, family members and all the other people we have relationship with and may have be in contact with.
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

DATA PROTECTION LAW

KERIC is following the European Union regulation about privacy and we want to assure people who come for activities organized by KERIC, employees, volunteers, partners from other organizations, local partners, family members and all the other people we have relationship with and may have be in contact with, that we care about their personal information responsibly. In relation to this general European General Data Protection Regulation (GDPR) an Act no. 18/2018 Coll.

The General Data Protection Regulations 2018 or GDPR describe how organisations must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The EU General Data Protection Regulation (GDPR) outlines six data protection principles that organisations need to follow when collecting, processing and storing individuals' personal data. The data controller is responsible for complying with the principles and must be able to demonstrate the organisation's compliance practices.
We've listed the six principles here with advice on how you can follow them.

1. Lawfulness, fairness and transparency
KERIC needs to make sure our data collection practices don't break the law and that they aren't hiding anything from data subjects.

2. Purpose limitation
KERIC should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.

3. Data minimisation
KERIC must only process the personal data that we need to achieve our processing purposes. Doing so has two major benefits. First, in the event of a data breach, the unauthorised individual will only have access to a limited amount of data. Second, data minimisation makes it easier to keep data accurate and up to date.

4. Accuracy

The accuracy of personal data is integral to data protection. The GDPR states that “every reasonable step must be taken” to erase or rectify data that is inaccurate or incomplete.

Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.

5. Storage limitation
KERIC needs to delete personal data when it’s no longer necessary. KERIC has right to store, collect and process and archive personal information personal information for accounting purposes for 10 years (based on Art. 431/2002 Coll accounting as amended) since the last implemented orders.

6. Integrity and confidentiality
This is the only principle that deals explicitly with security. The GDPR states that personal data must be “processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures”.

KERIC will ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates. We send name, address, email, phone, passport no, date of birth, info on any medical conditions, allergies, dietary requirements to host organisations and we share our Data protection policy and we ask them to follow it too.

THE DEFINITION OF PERSONAL DATA

The definition of personal data in the GDPR is broadened to include ‘any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.’

PEOPLE, RISKS AND RESPONSIBILITIES

POLICY SCOPE

This policy applies to:

- KERIC office
- All staff and volunteers of KERIC
- Host and partner organisations outside of European Economic Area we cooperate with (countries in Africa, Asia and Latin America etc.)
- All contractors, suppliers and other people working on behalf of KERIC

It applies to all data that the organization holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names and surnames
- Postal addresses
- Email addresses

- Telephone numbers
- Company name
- Any other information relating to individuals e.g. health information for overseas volunteers; or bank details for donors

DATA PROTECTION RISKS

This policy helps to protect KERIC from some very real data security risks, including:

- **Breaches of confidentiality,** for instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.
- **Administrative Penalty for Infringement of Articles.** Dependant on which article is infringed; the penalty can be up to 4% of annual global turnover or €20 million, whichever is greater.

RESPONSIBILITIES

Everyone who works and volunteers for or with KERIC has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and the GDPR principles.

However, these people have key areas of responsibility:

- The Data protection officer is **Statutory representative Miriam Petríková** is ultimately responsible for ensuring that KERIC meets its legal obligations. The responsibilities are mainly
    - Keeping the employees and volunteers and other people we cooperate with updated about data protection responsibilities, risks and issues.
    - Dealing with requests from individuals to see the data which KERIC holds about them (also called 'subject access requests').
    - Review all data protection procedures and related policies, in line with an agreed schedule.
        - Including ensuring that the data collected meets the standards for purpose limitations, data minimisation, and storage limitations.
    - Arrange data protection training and advice for the people covered by this policy in the organization.
    - Handle data protection questions from employees, volunteers and anyone else covered by this policy.
    - Check and approve any contracts or agreements with third parties that may handle the organization's sensitive data.
    - Ensure all systems, services and equipment used for storing data meet acceptable security standards.
    - Perform regular checks and scans to ensure security hardware and software is functioning properly.

- Evaluate any third-party services the organization is considering using to store or process data, for instance, cloud computing services.
- Implement a training schedule for all staff and volunteers that is appropriate for ensured compliance.
- Support host organisations to comply with Data Protection
- Approving any GDPR statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers and television.
- Current files secure in the main computer.

The **data processor- Ivana Hrušková** are responsible for:

- Keeping a record of all processing carried out on behalf of the data protection officer

KERIC will continue to monitor the data protection policy and compliance plan and issue recommendations for improvement and address any errors or gaps.

RIGHTS OF THE DATA SUBJECT

The GDPR give data subjects the following rights:

• To be informed that their data has been treated in a clear and understandable language.

• To have access to the data themselves.

• To rectify any erroneous or incomplete information.

• To oppose treatment on legitimate grounds.

• Not to be subject to an automatic decision to evaluate certain personal aspects, such as employment status, credit, reliability, and behaviour.

In addition, the Regulation on Data Protection (Regulation (EU) 2016/67923)[1], which was implemented from 2018 introduced:

• The right to forget. To request and obtain from those responsible, that their data be deleted when they are no longer necessary for the purpose.

• The right to portability. To request the transfer of your data to another responsible organisation of individual.

KERIC is required to:

[1] 23 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), http://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ES

• Ensure that rights are respected (i.e., by informing about and providing access to your data).

• Ensure that data are collected only for specific, explicit and legitimate purposes, which remain accurate and, where necessary, are updated for a period not exceeding that necessary.

• Ensure observance of data legitimacy criteria, for example, when a person gives consent, signs a contract, or has legal obligations, etc.

• Confidentiality in treatment.

• Safety in treatment.

• Notification to the data protection authority.

• Ensure that, when data transfer occurs to countries outside the EU, these countries ensure an adequate level of protection.

GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from the Data protection officer Miriam Petríková.
- KERIC will provide training to all employees and volunteers, to help them understand their responsibilities when handling data.
- Employees and volunteers should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the organization or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees and volunteers should request help from the data protection officer if they are unsure about any aspect of data protection.

DATA STORAGE

The GDPR requirements:

- Data to be stored with confidentiality and integrity secured including measures taken against accidental loss, destruction or damage
- Data protection officer (Miriam Petríková) retains a record of data processing activities. This must contain a specific set of information, so it is clear what is being processed, where it is processed, how it is processed and why it is processed
- Data processor (Ivana Hrušková) is required to keep a record of all processing carried out on behalf of the data controller

- These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data protection officer.
- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for or not electronical:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees and volunteers should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- Personal information is not left unattended and in clear view during the working day.
- The employees or volunteers do not take personal data home, all information is kept only in office.
- If some personal information is written on a scrub of paper and not needed anymore, we make sure it is disposed properly and as fast as possible.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by KERIC are entitled to:

- Ask what information the organization holds about them and why
- Ask how to gain access to it

- Be informed how to keep it up to date
- Be informed how the organization is following its GDPR obligations

If a person contacts the organization requesting this information, this request should by email, addressed to the data protection officer(Miriam Petríková) at mirka@keric.sk or keric@keric.sk.

The data protection officer will aim to provide the relevant data within 30 days or later in exceptional circumstances

The data protection officer will always verify the identity of anyone making a subject access request before handing over any information.

Data protection officer may refuse to release, delete data or limit access based on GDPR art.17 and 23 for these reasons:

- for exercising the right of freedom of expression and information (17.3.a)
- for the establishment, exercise or defence of legal claims (17.3.e)
- public security (23.1.c)
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions (23.1.g)

- the protection of the data subject or the rights and freedoms of others (23.1.i)
- the enforcement of civil law claims (23.1.j)

DATA BREACHES REPORTING

Data breaches must be reported to the data protection officer and the data subjects which they affect as fast as possible.

Data protection officer must inform the data protection processor about the breaches up to 72 hours.

Data breaches are to be reported via an incident form which must include measures being taken to address the breach and mitigate any possible side effects.

TRAINING AND REVIEW

Every long-term volunteer will receive a welcome package that will be informing them about all the policies that KERIC follows including Data Protection Policy.

Training for staff and long-term volunteers will be coordinated every 12 months.

This plan will be reviewed every 12 months

Self-assessment will be carried out annually

POLICY REVIEW

This policy was created in June 2019
This policy will be reviewed annually
In the event of new legislation passed into law while the current policy is active, the new legislative requirements will be added to and any conflicting procedures stated in this policy, will be deleted and the policy amended accordingly.

Next review date: June 2020