Data Protection Policy

Last updated	04/05/2020

Introduction

The purpose of the data collection/generation is related to the event “Present, in the Europe of the Future”, which is part of EUbyLakes project, co-funded by Europe For Citizens programme. (615617-CITIZ-1-2019-2-PT-CITIZ-NT).

The data which will be used to select applicants to the event, and to give and receive information from the project, namely through email.

The types and formats of data will be related to gathering information from forms: name, age range, gender, nationality, email, characterization of activity, interest in the project, others.

Online video sessions will be recorded and still pictures may be taken. These pictures and recorded video sessions can be made publicly available and/or shared through social media accounts related to current project and affiliated entities. Such media is not considered personal data.

This policy describes how this personal data is collected, handled and stored to meet the data protection standards — and to comply with the law, in particular GDPR.

Data protection principles

Data processing is in accordance with the responsibilities described under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. 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."

It applies to all data that held relating to identifiable individuals, namely:

a. Names of individuals
b. Nationality
c. Gender
d. Age range
e. Email addresses
f. Self-description provided by the participants

Data protection risks

This policy helps to protect from data security risks, including:

a. **Breaches of confidentiality.** For instance, information being given out inappropriately.
b. **Failing to offer choice.** For instance, all individuals should be free to choose how data relating to them is used.
c. **Reputational damage.** For instance, if hackers successfully gained access to data.

General staff guidelines

a. The only people able to access data covered by this policy are those who **need it for their work**.

b. Data **will not be shared informally**. When access to confidential information is required, employees can request it from their managers.

c. **Information is provided** to all employees to help them understand their responsibilities when handling data.

d. Employees will keep all data secure, by taking sensible precautions and following the guidelines below.

e. Personal data **will not be disclosed** to unauthorised people, either within the company or externally.

f. Data will 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.

g. Employees **will request help** from their manager or the data protection officer if they are unsure about any aspect of data protection.

Data minimisation

It is ensured that collected personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Subject access requests

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

a. Ask **what information** is held about them and why.

b. Ask **how to gain access** to it.

c. Be informed **how to keep it up to date.**

d. Right to **be forgotten**

e. Be informed how the company is **meeting its data protection obligations**.

If an individual requests this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed registration@eurolake.eu

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

Disclosing data for other reasons

In certain circumstances, GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, requested data will be disclosed. However, the data controller will ensure the request is legitimate, seeking assistance from the legal advisers where necessary.

Security

a. Personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions are be in place.

Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the risk to people's rights and freedoms shall be promptly assessed and report this breach, if appropriate.