QUEST POLICY ON DATA PROTECTION

CONTENTS

1. PURPOSE AND SCOPE

This policy provides a framework for ensuring that QUEST project meets its obligations under the General Data Protection Regulation (GDPR) and associated legislation.

It applies to all processing of personal data carried out for a QUEST purpose, irrespective of whether the data is processed on non-QUEST Consortium equipment or by third parties.

'Personal data' means any information relating to an identifiable living individual who can be identified from that data or from that data and other data. 'Processing' means anything that is done with personal data, including collection, storage, use, disclosure and deletion.

More stringent conditions apply to the processing of special category personal data.

'Special category' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

This policy does not cover the use of personal data by staff of the QUEST partners when acting in a private or non-QUEST capacity.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 824634

2. PRINCIPLES

The processing of personal data must comply with data privacy legislation and, in particular, the six data privacy principles of GDPR.

In summary, they require that personal data is:

• processed fairly, lawfully and in a transparent manner;

• used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;

• adequate, relevant and limited to what is necessary;

• accurate and, where necessary, up-to-date;

• not kept for longer than necessary; and

• kept safe and secure.

In addition, a new accountability principle requires QUEST to be able to evidence compliance with these principles.

3. AIMS AND COMMITMENTS

QUEST handles personal data and takes seriously its responsibilities under data privacy legislation. It recognizes that the mishandling of an individual's personal data may cause them distress or put them at risk of identity fraud. As a result, it is committed to:

• complying fully with data privacy legislation;

• adhering to good practice, as issued by the Data Protection Authorities of the QUEST Partners' countries and any other appropriate bodies;

• handling an individual's personal data in a careful and considerate manner that recognizes the importance of such information to their privacy and welfare.

QUEST seeks to achieve these aims by:

• ensuring that partners' staff and other individuals who process data for QUEST purposes are made aware of their individual responsibilities under data privacy legislation and how these apply to their areas of work;

• providing suitable training, guidance and advice;

• incorporating data privacy requirements into administrative procedures where these involve the processing of personal data, particularly in relation to major information systems (the principle of 'privacy by design');

• operating a centrally coordinated procedure (in order to ensure consistency) for the processing rights based requests made by individuals (eg. right of erasure);

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 824634

• investigating promptly any suspected breach of data privacy legislation; reporting it, where necessary, to the national Data Protection Authorities; and seeking to learn any lessons from the incident in order to reduce the risk of reoccurrence.

4. ROLES AND RESPONSIBILITIES

The Project Coordinator

The QUEST Project Coordinator has executive responsibility for ensuring that QUEST complies with data privacy legislation.

Information Compliance Team

The main contact for each partner institution, in collaboration with their own DPOs or equivalent are responsible for:

• establishing and maintaining policies and procedures in the consortium to facilitate the QUEST's compliance with data privacy legislation;

• establishing and maintaining guidance and training materials on data privacy legislation and specific compliance issues;

• supporting privacy by design and privacy impact assessments;

• responding to requests for advice from partners;

• coordinating a register to track the full range of processing that is carried out;

• complying with rights-based requests made by individuals;

• investigating and responding to complaints regarding data protection (including requests to cease the processing of personal data); and

• keeping records of personal data breaches, notifying the Data Protection Authorities of any significant breaches and responding to any requests that it may make for further information.

In fulfilling these responsibilities, they may also involve, and draw on support from, representatives from partners' offices, divisions, departments and units.

Project Management Board

The QUEST Project Management Board is responsible for ensuring that the processing of personal data related to QUEST activities in their organization conforms to the requirements of data privacy legislation and this policy. In particular, they must ensure that:

• new and existing staff, visitors or third parties associated with their institution who are likely to process personal data are aware of their responsibilities under data privacy legislation. This includes drawing the attention of staff to the requirements of this policy, ensuring that staff who have responsibility for

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 824634

handling personal data are provided with adequate training and, where appropriate, ensuring that job descriptions for members of staff or agreements with relevant third parties reference data privacy responsibilities;

• adequate records of processing activities are kept (for example, by undertaking register exercises);

• data protection requirements are embedded into systems and processes by adopting a 'privacy by design' approach and undertaking privacy impact assessments where appropriate;

• privacy notices are provided where data is collected directly from individuals or where data is used in non-standard ways;

• data sharing is conducted in accordance with QUEST coordinator guidance;

• requests from the Information Compliance Team for information are complied with promptly.

Others processing personal data for a QUEST purpose e.g. staff, participants to events, etc.

Anyone who processes personal data for a QUEST purpose is individually responsible for complying with data privacy legislation, this policy and any other policy, guidance, procedures, and/or training introduced by QUEST partners to comply with data privacy legislation. In summary, they must ensure that they must ensure that they:

• only use personal data in ways people would expect and for the purposes for which it was collected;

• use a minimum amount of personal data and only hold it for as long as is strictly necessary;

• keep personal data up-to-date;

• keep personal data secure, in accordance with the QUEST's Information Technology Security Measures;

• do not disclose personal data to unauthorized persons, whether inside or outside the QUEST consortium;

• complete relevant training as required;

• report promptly any suspected breaches of data privacy legislation, in accordance with the procedure in section 6 below, and following any recommended next steps;

• seek advice from the Information Compliance Team where they are unsure how to comply with data privacy legislation; and

• promptly respond to any requests from the Information Compliance Team in connection with subject access and other rights based requests and complaints (and forward any such requests that are received directly to the Information Compliance Team promptly).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 824634

5. BREACHES OF DATA PRIVACY LEGISLATION

QUEST will investigate incidents involving a possible breach of data privacy legislation in order to ensure that, where necessary, appropriate action is taken to mitigate the consequences and prevent a repetition of similar incidents in future. Depending on the nature and severity of the incident, it may also be necessary to notify the individuals affected and/or the Data Protection Agency. A breach will occur where, for example, personal data is disclosed or made available to unauthorized persons or personal data is used in a way that the individual does not expect.

All other incidents must be reported directly to the DPO of the interested partner at the earliest possible opportunity and to the project coordinator.

6. COMPLIANCE

QUEST regards any breach of data privacy legislation, this policy or any other policy and/or training introduced by QUEST partners from time to time to comply with data privacy legislation as a serious matter, which may result in disciplinary action. Depending on the nature of the breach, an individual may also find that they are personally liable (for example, it can be a criminal offence for a partner of QUEST to disclose personal information unlawfully).

7. FURTHER INFORMATION

Questions about this policy, data privacy matters in general and information security should be directed to the QUEST Scientific coordinator at:

ilda.mannino@univiu.org

8. REVIEW AND DEVELOPMENT

This policy, and supporting guidance, will apply with effect from 1 March 2019. Any revisions or updates will be published on the QUEST website.

9. RELATED POLICIES AND NOTICES

This policy should be read in conjunction with related policies and regulations in act at the different partners' organization.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 824634