eGRiST Data Protection Impact Assessment (DPIA) Summary

A DPIA is a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. DPIAs are required under the UK General Data Protection Regulation (UK GDPR).

DPIAs aid us in determining how a particular project, process or system may affect the privacy of an individual. They allow organisations to identify and mitigate risks when processing data and to understand how to design more effective processes for handling personal data.

We have followed the principle of data protection by design and by default from the early stages of eGRiST. The data we collect is pseudonymised and we do not store personal identification information. However, our GDPR compliance review highlighted some aspects of the data which required documentation. We determined that a DPIA was needed for eGRiST because:

1. We process special category data regarding mental health assessments.
2. Our system performs some simple, automated processing which is a type of profiling.
3. Our assessment data can be for children and vulnerable individuals.
4. Our assessment data is collected by users of our system who are mental health professionals. The data subject's relationship is with our user, not directly with us.
5. We archive data for future research and development to help us better analyse and understand mental health risk assessment and improve the capabilities of our system for future users.

Recommendation and Conclusion

Risks were documented regarding these aspects of our data processing and other, wider implications for data security and privacy.

All data subjects are considered vulnerable if they are being assessed for mental health difficulties; the principles of data protection by design and by default are therefore built into the system.

We do not use the data for any other reason than for which it was collected and we do not transfer data anywhere else.

Appropriate technical and organisational measures have been implemented to protect individuals and their rights. Data minimisation principles are employed. No identification information is stored with the assessment data; the system uses pseudonymous links which are fully severed if the data is archived.

The system performs some simple, automated processing to format and structure the evaluation report but it does not automate decision-making. The processing does not make decisions about data subjects that have a legal or similar effect on them. Mental health professionals oversee assessments; they are responsible for any subsequent decisions and management plans.

All risks were found to have been reduced to acceptable levels by existing controls and privacy by design principles.

The current DPIA was signed off by our DPO and SIRO on 25th July 2022.

Prior consultation with the ICO was concluded to not be required.

The DPIA is reviewed annually and available on request.