GHGA

THE GERMAN HUMAN GENOME-PHENOME ARCHIVE

Research Data Protection and Data Sharing via GHGA

Simon Parker, Data Protection Coordinator

RDM and Data Protection

- Research Data Management focuses on the collection, cleaning, labelling, storage, and management of access to research data.

- When working with data about people, there is also a need to consider applicable data protection law.

- The areas we'll be looking at today are:
  - Whether you have personal data?
  - What your role is?
  - What is your justification for processing?
  - What other obligations you have.

- I will be using examples from GHGA to explain how we have put these concepts into practice.

Introduction to GHGA

- The German Human Genome-phenome Archive is an NFDI-funded project to create a national archive for human omics research data.
- We will be launching our Archive soon, with a Cloud phase to follow.
- 22 institutions from across Germany are involved in the project. 7 institutions are planned to operate Data Hubs, and will be storing omics data.
- Metadata is currently being made publicly available to improve the findability of the omics data.

GHGA

THE GERMAN HUMAN GENOME-PHENOME ARCHIVE

Do you have personal data?

Personal Data

- Information that relates to an identified or identifiable natural person. That person has to be living* (Article 4). Referred to as a Data Subject.
- The ability to (re-)identify a person is crucial as to whether the GDPR is applicable.
- Identification can be direct or indirect; indirect identification will typically use multiple pieces of information in combination.
- The likelihood of identification must be reasonable (Recital 26).

Source: artic.edu

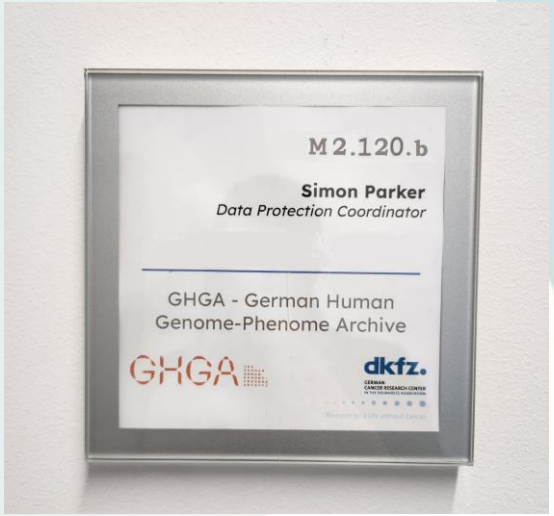
Direct and Indirect Identification

Name	Office	Position	Age	Nationality	Annual Salary
Simon Parker	M2.120.b	Data Protection Coordinator	25	British	22€

Direct Identification

Office	Position	Annual Salary
M2.120.b	Data Protection Coordinator	22€

Indirect Identification



Are some data more sensitive?

- The GDPR specifies that certain types of data, or data about specific topics is more sensitive than other forms of personal data (Article 9).

- This is because they concern topics that are likely to be sensitive to people, or because there is an increased risk that they can be used to re-identify someone.

- These are termed ‘special categories of personal data’ and there are additional restrictions around the processing of these.

- There are 8 categories of data described as special category: racial or ethnic origin, political opinions, religious or philosophical beliefs, sexuality and sex life, genetic data, biometric data, trade union memberships, data about health.

GHGA Data Types

- Early in the project, we defined the different data types that we would be processing.

- Three data types:
  - Research Data – Omics data. Special category personal data.
  - Metadata – Describes Research Data. Can be personal or non-personal.
  - Administrative Data – Generated through the operation of the infrastructure. Can be personal data.

- Having defined the data to be processed, we could assign GDPR roles to all of the parties involved for each data type.

GHGA

THE GERMAN HUMAN GENOME-PHENOME ARCHIVE

What is your role?

Controller and Processor

- Two of the key roles defined in the GDPR are Controllers and Processors.
- A Controller is a natural or legal person, who is responsible for defining the purposes and means of data processing.
- A Processor processes data on behalf of a Controller.
- Data processing may have multiple Controllers if the purpose and means of processing have been defined jointly.

GHGA Roles

- In addition to defining roles, we also wanted to minimise the number of parties within GHGA who have access to personal data.

Data Type	Roles
Administrative Data	GHGA institutions who require access will be Joint Controllers.
Non-personal Metadata	Outside of GDPR so no Controller required.
Personal Metadata	The Submitter is the Controller. GHGA will be the processor.
Research Data	The Submitter is the Controller. GHGA will be the processor.

GHGA

THE GERMAN HUMAN GENOME-PHENOME ARCHIVE

What is your justification for processing?

Legal Bases

- The GDPR prohibits data processing, unless it is lawfully justified.
- The legal bases provide us with a lawful justification for that processing to take place.
- The legal bases for processing personal data are listed in Article 6 (1).
- When processing a special category of personal data, a legal basis is also needed under Article 9 (2) in addition to a legal basis under Article 6 (1).

GHGA

Article 6

Consent (a)	The data subject has given consent to the processing of their personal data.
Contract (b)	Processing is necessary for the performance of a contract.

Legal Obligation (c)	Processing is necessary for compliance with a legal obligation.
Vital Interests (d)	Processing is necessary in order to protect the vital interests of the data subject.

Public Task (e)	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
Legitimate Interest (f)	Processing is necessary for the purposes of legitimate interests pursued by the controller.

Article 9

- When processing a special category of personal data, a legal basis described under Article 9 is also required.
- Article 9 (2) lists 10 legal bases for processing.
- (a) consent; (j) archiving/scientific/research purposes.
- (b) employment and social security law; (c) vital interests of the Data Subject; (d) political, philosophical, religious, or trade union aims; (e) made public by the Data Subject; (f) legal defence; (g) substantial public interest; (h) preventative or occupational medicine; (i) public health.

Consent

- Consent can be a legal basis under Article 6 and Article 9.
- Consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes.
- The consent has to be recorded and monitored to ensure that it remains valid – a Data Subject has the right to withdraw their consent at anytime.
- It can be a particularly useful legal basis when sharing personal data between EU/EEA countries.

GHGA's Legal Bases

- There are different legal bases for the different data types processed by GHGA. The legal basis will also vary depending on how the data are collected.

Data Type	Legal Basis
Administrative Data	6 (1) a – Consent Surveys, community engagement etc. 6 (1) b – Contract Personal data collected through our contracts. 6 (1) f – Legitimate Interest Helpdesk
Non-personal Metadata	Outside of GDPR so no legal basis required.
Personal Metadata	The Controller is responsible for defining the legal basis.
Research Data	The Controller is responsible for defining the legal basis.

GHGA

THE GERMAN HUMAN GENOME-PHENOME ARCHIVE

What are your other obligations?

General Principles in the GDPR

Data minimisation - Only the data that is required and necessary to achieve the objectives of the proposed processing should be collected.

Pseudonymisation and Anonymisation - Whenever possible, personal data should be processed in such a way as to minimise the risk of disclosure. This may include the replacement of direct IDs with pseudonyms or other techniques that render the data as non-personal.

Security standards - Appropriate security measures should be in place to protect personal data. This may include access controls, encryption, or technical processing restrictions. This is particularly important for sensitive personal data.

Data Subjects' Rights

- Data Subjects retain certain rights regarding their personal data. These require data controllers to meet certain information obligations and permits Data Subjects to influence the ways in which their data are processed.

- Article **13 and 14** → the right to **be informed** about the processing.
- Article **15** → the right to **access data** and other related information.
- Article **16** → the right to **have errors rectified**.
- Article **17** → the right to **be forgotten**.
- Article **18** → the right to **restrict** processing.
- Article **21** → the right to **object**.

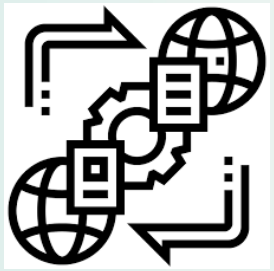
GHGA

RoPAs and DPIAs

- When processing personal data, Controllers and Processors should maintain a **Record of Processing Activities** describing the data processing they are responsible for (Article 30).
  - Name and contact details of the Controller, the processing purpose, the categories of the Data Subjects and the personal data, recipients of the data, time limits for the erasure, and TOMs.
  - Your institutions will usually have a mechanism for registering processing activities.

- **Data Protection Impact Assessments** are performed when the proposed processing of personal data is likely to lead to a higher risk to the Data Subjects (Article 35).
  - A threshold analysis can be performed to assess whether a DPIA is required.
  - DPIAs should assess the risks to the rights and freedoms of the Data Subjects and how the safeguards in place will reduce those risks.

International Transfers



- Transfers between countries which are subject to the GDPR are permitted. However, the legal basis for the processing in the sending country must also be legally implemented in the destination country.
- Transfers to third countries or international organisations can be permitted when safeguards are in place: including adequacy decisions, standard contractual clauses, and binding corporate rules. There may be some exceptions in specific circumstances.
- The USA does not have a full adequacy decision with the EU. The UK does as it continues to implement legislation similar to the GDPR.

GHGA's Data Protection Documents

- Records of Processing Activities (RoPA)
  - Administrative Data, Helpdesk, Research Data and Personal Metadata, Website, Surveys
  - Administrative Data, Research Data and Personal Metadata

- Technical and Organisational Measures
  - GHGA's TOMs are used to define the measures that are in place to protect the data processed.
  - Basic Measures, Measures for Confidentiality, Encryption and Pseudonymisation, Measures for Integrity, Measures for Availability, Resilience, and Recoverability, Procedures for Regular Review, Assessment, and Evaluation, and Technology.

- Data Protection Impact Assessments
  - DPIAs were not required for Administrative Data.
  - We have worked on performing a Risk Assessment for Research Data and Personal Metadata which will be made available to Data Controllers.

Summary

- When planning how to handle data for research purposes, it is important to consider whether data protection legislation applies.
- You should always consider whether the data you are processing meets the definition of personal data as described in the GDPR.
- If you are processing personal data, you should consider whether you are doing so as controller or a processer, and what the legal basis that justifies that processing is.
- Finally, you must ensure that you are meeting your legal obligations such as completing a RoPA describing the processing you will do, and if necessary, a Data Protection Impact Assessment.
- If you are currently generating human omics data, perhaps consider sharing via GHGA.

Thank you for listening

For further information about GHGA, please see our website

www.ghga.de