GHGA

THE GERMAN HUMAN GENOME-PHENOME ARCHIVE

An Introduction to Data Protection

Simon Parker, Data Protection Coordinator

Introduction

- The purpose of this course is to give you an overview of data protection law, primarily the GDPR.

- We will be covering five areas, with time for discussion around the issues raised.

- We will reference the legal text when relevant but not go into the details unless it is essential to do so.

GHGA

Learning Objectives

- Understand what is meant by personal data, and why some personal data are categorised as ‘special category’.
- Awareness of the role of legal bases in personal data processing and what the legal bases are.
- Knowledge of the different roles in personal data processing and what obligations they have.
- Know what rights Data Subjects have, and how they are exercised.
- Understand how personal data is protected in GHGA.

GHGA

Part 1

What is personal data?

Intro to the GDPR

- The General Data Protection Regulation (GDPR) is the main data protection legislation across the EU and EEA. It applies to data about EU and EEA citizens wherever their data is processed.

- It was adopted in April 2016 and came into force in May 2018.

- The GDPR is directly binding and applicable, although there is some flexibility to adapt some aspects of the regulation in Member State law.

- In Germany, it is implemented at a federal level via the DSGVO and within the data protection legislation of each federal state.

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).

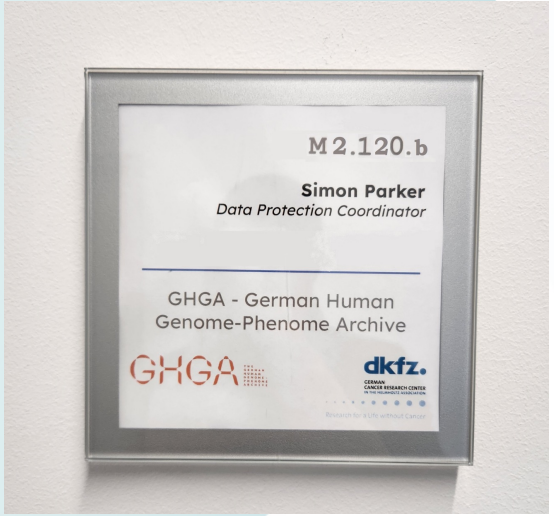
Direct and Indirect Identification

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



GHGA

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.

Which of these is a special category?

Racial or ethnic origin

Criminal convictions

Political opinions

Religious or philosophical beliefs

Marital status

Sexuality and sex life

Images

Income

Genetic data

Biometric data

Educational attainment

Employment history

Trade union memberships

Data about health

GHGA

Anonymisation and Pseudonymisation

- Anonymisation and pseudonymisation are methods to reduce the potential for data to be used to identify a Data Subject.

- Anonymisation refers to the process of manipulating personal data such that is no longer personal. This can be done by removing directly identifying information, aggregating, suppression, or other similar techniques.

- Pseudonymisation is the process of removing directly identifiable information from a dataset. Typically this will involve replacing such data with pseudonyms. Pseudonymised data may still be considered to be personal depending on whether other protections are in place.

General Principles

- *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.

Section Summary

- In this section we have looked at what is meant by personal data under the GDPR.
- We have seen the difference between direct and indirect identification.
- We have also discussed what data types are considered to be more sensitive.
- Finally, we have learned about the difference between anonymisation and pseudonymisation.

Part 2

What are the legal bases for processing?

Can we process personal data?

- The GDPR considers any action that is performed on personal data to be ‘processing’ of that data (Article 1).

- Processing does not mean just ‘using’ the data for a particular purpose. Collection and storage, even if automated, would still be considered a form of data processing.

- The processing of personal data is forbidden by the GDPR, unless certain conditions are met.

- These conditions include the legal bases for processing.

Legal Bases

- One of the key requirements of the GDPR is that any processing of personal data is 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).

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.

GHGA

Pick a legal basis

A patient has been brought into a hospital unconscious. A person with them is able to provide information so that they can be identified and their medical record accessed.

What would be a suitable legal basis for processing?

Consent | Contract | Legal Obligation | Vital Interests | Public Task | Legitimate Interest

Pick a legal basis

A research project is collecting personal data from survey participants so that they can contact them afterwards for a follow-up interview.

What would be a suitable legal basis for processing?

Consent | Contract | Legal Obligation | Vital Interests | Public Task | Legitimate Interest

Pick a legal basis

A charity wishes to use data collected by a public authority about local residents in order to tackle a particular issue. It would not be possible to speak directly to residents due to budgetary and time constraints.

What would be a suitable legal basis for processing?

Consent

Contract

Legal Obligation

Vital Interests

Public Task

Legitimate Interest

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.
- It is also an available legal basis for a transfer to another EEA country.
- 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.

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 an adequacy decision with the EU. The UK does as it continues to implement the GDPR.

Section Summary

- In this section, we looked at the legal bases for processing.
- A legal basis is required to process personal data under Article 6, and another under Article 9 if processing special category data.
- We identified the legal bases that are most likely to relevant in a research project.
- We also discussed consent as a legal basis and the challenges associated with international transfers.

Part 3

What are the roles in data processing?

Controller and Processor

- Two of the key roles defined in the GDPR are Controllers and Processors.
- A Controller 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.

Choose the Correct Role

A research institute is generating large amounts of personal data from study participants. They have decided to outsource the creation of the infrastructure they will use to process the data to an external party. What is the GDPR role of the external party?

Controller

Processor

Joint Controller

Choose the Correct Role

Researchers at two universities have designed a project that will process personal data. One of the universities will collect the data, but the analysis will be performed at the other. What is the GDPR role of the first university?

Controller

Processor

Joint Controller

Choose the Correct Role

A research institute has been recruited by a hospital to conduct analysis on their patients' data, as they wish to better understand the effectiveness of the treatments they offer. The research institute has a relationship with a local university and asks them to support their work. What is the GDPR role of the research institute?

Controller

Processor

Joint Controller

Data Protection Officer

- The GDPR requires a Controller and Processor to designate a Data Protection Officer when their core activities involve the processing of special category data. There may also be requirements in Member State law to designate a DPO for other forms of processing.

- A Data Protection Officer has the responsibility of providing independent oversight of processing. Their tasks are defined as:
  - informing and advising controllers or processors;
  - monitoring compliance with law and providing awareness training;
  - providing advice regarding DPIAs;
  - cooperating with the supervisory authority;
  - acting as a contact point for the supervisory authority.

Section Summary

- In this section we have looked at some of the different roles that are defined in the GDPR.
- We have seen the differences between Controllers and Processors and how to decide which role is most appropriate.
- Finally we have seen the responsibilities that a Data Protection Officer has.

Part 4

What rights do Data Subjects have?

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 obligation to provide information about the processing.

- Article 15 - the right to access data and other related information.

- Article 16, 17, 18, and 21 - the right to have errors rectified, the right to be forgotten, the right to restrict processing, the right to object.

Articles 13 and 14

- Articles 13 and 14 require Controllers to provide information about the processing they are doing to the Data Subjects.

- Article 13 covers data that is collected from the Data Subject directly, whereas Article 14 covers data is collected from other sources.

- The Controller must make the Data Subjects aware of:
  - the identity and the contact details of the Controller;
  - the contact details of the DPO;
  - the purposes of the processing and the legal basis;
  - who the data will be shared with;
  - how long the data will be stored;
  - what their rights and how they can be exercised.

- Typically this information is provided via consent information or a privacy notice or statement.

GHGA

Article 15

- Article 15 describes a Data Subject's right to access information about them that is being processed by a Controller.

- Data Subjects have the right to receive a copy of the data about them that the Controller has. Article 20 states this must be in a structured, commonly used, and where possible machine-readable, format.

- Alongside the data, the Controller must also provide information regarding:
  - the purposes of the processing;
  - the categories of personal data being processed;
  - the recipients to whom the personal data will be disclosed;
  - the envisaged period storage period;
  - information about the right to request rectification, erasure, the restriction of processing or to object;
  - where the Controller obtained the data;
  - if the data are being used for automated decision-making.

- This right is not absolute, if access to the data impacts the rights and freedoms of others it may be prohibited.

GHGA

Articles 16 and 18

- Article 16 gives Data Subjects the right to rectification. If personal data about them is incorrect, the Data Controller is obliged to correct it.

- Article 18 is the right to restrict processing. This is often used alongside Article 16; a Data Subject can request that their data is not processed until it is rectified.

- Other reasons for a restriction include:
  - the processing is unlawful but the Data Subject opposes the deletion of the data;
  - the data are no longer required by the Controller, but they are required by the Data Subject as part of legal claims;
  - the Data Subject has objected to processing pursuant to Article 21(1).

GHGA

Articles 17 and 21

- Article 17 is the right to erasure, sometimes referred to as the right to be forgotten.

- Data Subjects can request that the Controller erase personal data held about them.

- This can be requested under a number of conditions including:
  - the personal data are no longer required for the reason they were collected;
  - the Data Subject withdraws their consent;
  - the Data Subject objects to the processing under Article 21;
  - the personal data have been processed unlawfully.

- Article 21 gives Data Subjects the right to object to processing.
  - It is applicable if processing is based on 6(1) e or 6(1) f.
  - The Controller has to demonstrate why they have a compelling reason to continue processing.

GHGA

Match the Articles

Article	Right
13	
14	
15	
16	
17	
18	
21	

To information

To erasure

To restrict

To rectification

To access

To object

To information

Section Summary

- In this section we have looked at some of the key rights that Data Subjects have with regards to the processing of their personal data.
- Controllers are obliged to provide information to Data Subjects so that the data processing is transparent.
- Data Subjects can request access to their data and copies of it, and can have errors rectified.
- They can also request that a Controller stops processing their data for various reasons.

Part 5

Data Protection with GHGA.

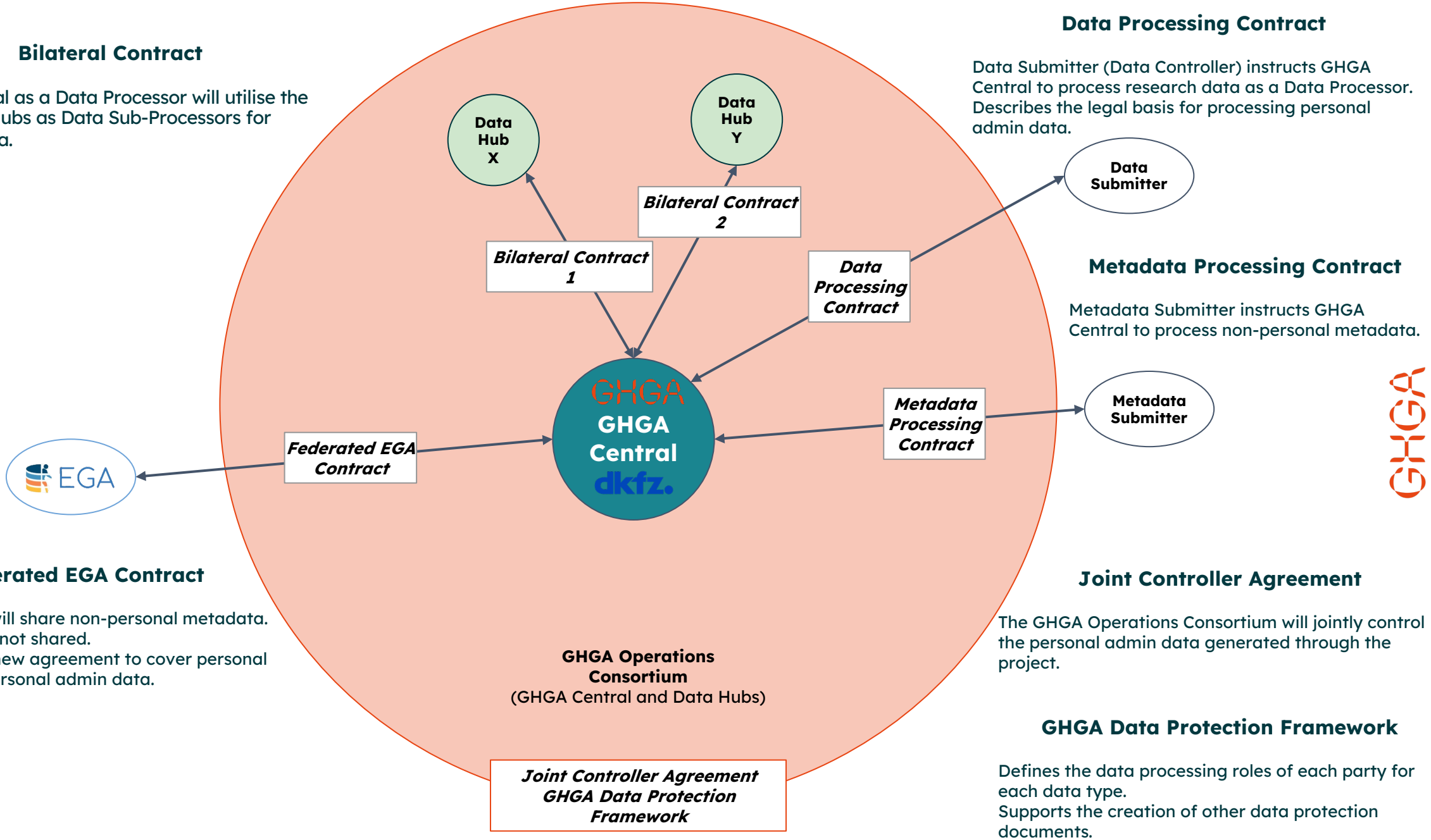
Our Data Types

Administrative Data	Data which is generated as part of the operation of the GHGA project. This includes information about Data Submitters and Requesters, members of staff, Service Users, and the research community. Processing is performed under 6(1) a, 6(1) b, and 6(1) f.
Metadata	Non-personal Metadata is any information that describes Research Data but which is non-personal according to Recital 26. This is typically collected via the GHGA metadata submission spreadsheet and is made available via the Catalog/Portal. Personal Metadata is any information that describes Research Data but that would be considered personal according to Recital 26. It is also likely to be a special category of personal data as it relates to health. This will be submitted alongside the Research Data. Processing performed under the legal basis of the Data Submitter.
Research Data	Research Data is the omics data submitted for archiving by Data Submitters. It is a special category of personal data. Processing is performed under the legal basis of the Data Submitter.

GHGA

Bilateral Contract

GHGA Central as a Data Processor will utilise the other Data Hubs as Data Sub-Processors for research data.



Data Processing Contract

Data Submitter (Data Controller) instructs GHGA Central to process research data as a Data Processor. Describes the legal basis for processing personal admin data.

Metadata Processing Contract

Metadata Submitter instructs GHGA Central to process non-personal metadata.

Federated EGA Contract

EGA and GHGA will share non-personal metadata. Research data is not shared.
Option to add a new agreement to cover personal metadata and personal admin data.

Joint Controller Agreement

The GHGA Operations Consortium will jointly control the personal admin data generated through the project.

GHGA Data Protection Framework

Defines the data processing roles of each party for each data type.
Supports the creation of other data protection documents.
Describes the legal bases for the work.

Key Documents

- Records of Processing Activities (RoPA)

  When processing personal data, it is necessary to record the processing purpose, why the data are being processed, and who is doing the processing etc.

- Technical and Organisational Measures

  TOMs are a high-level description of the protections that are in place to protect personal data. This includes physical measures, IT policies, and standard operating procedures.

- Data Protection Impact Assessments

  DPIAs are performed by Controllers when they are processing data in a manner that is likely to result in a higher risk to Data Subjects. These risks have to be identified and TOMs aligned to them as mitigations.

GHGA

Key Policies

- Data used within the GHGA project must on be stored in approved systems and only accessed by approved people.
- Approved systems are those described in RoPAs and TOMs.
- Access is role-specific. It is also necessary to ensure that there is a suitable legal basis for the processing – not all institutions in the GHGA Consortium have been approved to process data.
- When in doubt, it is better to ask!

Data Breaches

- Within GHGA we have defined two forms of breach:
  - **Data Breach**: where ‘there has been the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed’ as outlined by Art. 4 GDPR.
  - **Procedural Breach**: where data has been handled contrary to our policies but not such that it reaches the level of Data Breach.
- It is important to act quickly. We have to notify the Controller within 24 hours of a breach being discovered.
- The DPO will be heavily involved in resolving any breaches, but we will be expected to support their efforts.
- All breaches are recorded internally so that we can improve.

GHGA

Data Subject Rights

- Data Subjects may ask to exercise their rights by contacting GHGA Central, the DPO at the DKFZ, or the DPO at one of the Data Hubs.
- Requests that are sent into the Helpdesk should be passed on to the Data Protection Coordinator or Helpdesk Lead.
- GHGA is unable to act for the Research Data and Personal Metadata. These requests will have to go to the Controller.
- GHGA may have to act if the request relates to Administrative Data. In such cases, the DPO at the DKFZ will coordinate efforts.

Section Summary

- In this section we have looked at some of the features of GHGA's data protection concept.
- We have seen the data types that we will be processing and the key documents that govern how we do so.
- We have also explored how these documents fit together so that we can provide an service to our users.
- Finally, we have seen how we handle data breaches and data subjects' requests.

GHGA

Questions

Do you have any questions about what we have covered today?

Thank you for listening