PhenoMeNal Terms of Use version 1.1 (Last update: 31/07/2018)

1. **Definition of terms used in this document**

Anonymisation
Data are considered to be anonymised where they are fully (unlinked) anonymised or linked (coded, pseudo-) anonymised where the linkage code (cipher) is not held by, or accessible to, the researchers/research establishment. 'Anonymised' data do not contain any identifiable information such as, for example, name, address, phone number, full date of birth, national health or social insurance numbers, full postcode, etc., and it is not reasonably possible for the researcher to identify the individual to whom the data relate.

Linked anonymised (or pseudoanonymised or coded) data are fully anonymous to the researchers who receive or use them, but contain information or codes that would allow others (e.g., the clinical team who collected them or an independent body entrusted with the safekeeping of the code) to link them back to identifiable individuals.

Unlinked anonymised data contain no information that could reasonably be used by anyone to identify the individuals who donated them or to whom they relate.

Data
The term 'data' in this document may refer to genomic data, anonymised images, metadata, etc. It does not refer to data that contains identifiable information such as name, phone number, or date of birth.
Personal Data
Data which may be used to identify a research participant. (Note: although in some EU jurisdictions personal data may also be used to describe human biosamples, in the context of this document, it relates to identifiable data only).

Data provider
The 'data provider' is the individual researcher or investigator or body of researchers or investigators that makes data available for access and use within the Phenomenal project. (It does not refer to the participant.)

Data User
The 'data user' is the individual researcher or investigator or body of researchers that processes data through the Phenomenal software and infrastructure.

Data Controller
The organisation which determines the purposes and means of processing personal data.

Data Processor
The organisation which processes data on behalf of the data controller.

GDPR

General Data Protection Legislation

2. Project Aims

PhenoMeNal is an integrated, secure, on-demand service-driven, privacy-compliant and sustainable European e-infrastructure for processing, analysis and information-mining of metabolomics data. The project has been designed to enable maximum benefit from research by making data as accessible as possible to the research community, while protecting the interests of participants from whom the data originate with regard to Ethical, Legal and Social Implications (ELSI) and within the scope of their consent. These Terms of Use reflects PhenoMeNal's commitment to provide this service and impose no additional constraints on the use and transfer of the contributed data than those provided by the data owner.

3. Data Providers and users of Phenomenal

Data providers and users of Phenomenal have a number of responsibilities and obligations, such as the obligation to respect participant confidentiality. Researchers accessing the data have a custodian role, to ensure the careful and responsible management of the information. They have an obligation to operate in conformity with the requirements of their own institution and fulfil all necessary national and international regulatory and ethical requirements such as the General Data Protection Regulations (GDPR). They also have obligations to the PhenoMeNal project, the integrity of their own research, as well as the funders and the wider research community, to carry out high quality, ethical research.

4. Project Specific considerations

Consideration should be given to Ethical Legal and Social Implications for handling data within the project with respect to:

- Trans-border/international access to data
- Establishment of new links between data or types of data that were not linked before.

5. Terms of use of Phenomenal Infrastructure and Software

- All users have an obligation of confidentiality and must conform to data protection principles to ensure that data is processed in compliance with the legal and ethical requirements.
- The data owners must ensure that they have sought and obtained, where necessary, all appropriate approvals, ethical and legal, for the data collected.
- For animal data, the data owner must ensure that national guidelines for their welfare and care during the collection of data has been followed.

- PhenoMeNal does not guarantee the accuracy of any provided data.
- PhenoMeNal has implemented appropriate technical and organisational measures to ensure a level of security which we deem appropriate, taking into account the sensitivity of data we handle. However, the data provider holds sole responsibility for the usage and distribution of data.
- Computing of personal and sensitive data on PhenoMeNal infrastructure should be run internally by the users on their secure infrastructures behind appropriate firewalls. PhenoMeNal will not hold any liability for any loss or damage to data.
- While we will retain our commitment to privacy of sensitive data, we reserve the right to update these Terms of Use at any time. When alterations are inevitable, we will attempt to give reasonable notice of any changes by placing a notice on our website, but you may wish to check each time you use the website. The date of the most recent revision will appear on this, the 'PhenoMeNal's Terms of Use' page. If you do not agree to these changes, please do not continue to use our services. We will also make available an archived copy of the previous Terms of Use for comparison.
- The Phenomenal development team reserve the right to make changes to the software at any time.
- Background information on the General Data Protection Regulations is in the attached Appendix.
- Any questions or comments concerning these Terms of Use can be addressed to: PhenoMeNal-help@ebi.ac.uk

6. Confirmation of Acceptance of the terms of Use

Data providers and data processors certify that they will abide by this Ethical Governance Framework, Terms of Use and its stipulations, and that appropriate ethical approval and/or consent are in place prior to use of the data within their project. The acceptance of these conditions along with other registration data will be collected by the project coordinator and stored centrally. During registration you will be asked (yes/no) if you accept the terms and conditions.

You will be asked to provide your name, address, organisation, email address and contact phone number. During registration we will ask for your consent (yes/no) to use this information under the General Data Protection Legislation which was introduced on the 25th May 2018 in the European Union. This information will be

used to contact users of PhenoMeNal, supply information on updates to the software and to monitor use of the software.

Appendix

Background information on the GDPR legislation

Introduction

On the 25th May 2018, the new European data protection legislation comes into force.

The General Data Protection Regulation, known as GDPR, (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679) is the most significant data protection legislation to be introduced in the past 20 years and will replace the 1995 EU Data Protection Directive. The key changes are set out below.

In the context of Phenomenal, the GDPR will apply to identifiable, or pseudo anonymised personal data, which could include metabolomics data. Completely non-identifiable anonymised data is outside of the scope of the GDPR.

The publicly available implementations of Phenomenal should therefore only use non-identifiable anonymised data. There may be circumstances where Phenomenal is implemented by an organisation and use identifiable or pseudo anonymised data e.g. behind an institutional firewall in a secure environment. In this case, local regulations, consent and permissions to store and process the data should be taken into account as GDPR will apply.

The GDPR – key changes

The aim of the GDPR is to protect EU citizens from privacy and data breaches. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR can be found below.

For the purposes of the description, we define a Controller and Processor as:

- **Data Controller** – The organisation which determines the purposes and means of processing personal data.
- **Data Processor** – The organisation which processes data on behalf of the data controller.

1. Increased Territorial Scope (extra-territorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies/organisations/persons processing the personal data of data subjects residing in the Union, regardless of the location. Previously, territorial applicability of the directive was ambiguous and referred to the data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GDPR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-Eu businesses/organisations processing the data of EU citizens will also have to appoint a representative in the EU.

2. Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious

infringements e.g. not having sufficient consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. an organisation can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting an impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

3. Consent

The conditions for consent have been strengthened, and companies/organisations will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

4. Data Subject Rights

a. Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers and the controllers, "without undue delay" after first becoming aware of a data breach.

b. Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

c. Right to be forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

d. Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a '*commonly use and machine readable format*' and have the right to transmit that data to another controller.

e. Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - *'The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'.* Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

5. Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.

6. Summary

In summary, GDPR is designed to strengthen the rights of individuals regarding their personal data and is intended to unify data protection laws across Europe. These laws are intended to protect EU citizens and will apply regardless of where a user's data is processed. Phenomenal is committed to GDPR compliance.

7. **How will GDPR impact use of Phenomenal?**

The extent to which GDPR will impact you will depend in part on the way in which Phenomenal is deployed and used in your organisation. This is because GDPR makes a distinction between two types of roles:

- **Data Controller** – The organisation which determines the purposes and means of processing personal data.
- **Data Processor** – The organisation which processes data on behalf of the data controller.

Firstly you must identify who owns the roles of Data Controller and Data Processor based on how Phenomenal is deployed. These are:

- **On Premise** – In this scenario Phenomenal software is installed and run on servers within your own organisational control. For the purposes of GDPR your organisation will most likely (unless you outsource the administration of the servers or the day to day running of your software) be both the Data Controller and the Data Processor.
- **Non EMBL-EBI supplied Cloud** – In this scenario Phenomenal is installed and run on servers hosted in an external data centre. For the purposes of GDPR your organisation may (intentionally or unintentionally) split the duties, roles and responsibilities of Data Controller and Data Processor with the company who manages your hosted environments. A further complication may arise when the company who manages your environment is themselves using the services of 3rd party SAAS and IAAS providers (for example Microsoft, Amazon or Google).
- **PhenoMeNal in the EMBL-EBI EMBASSY Cloud** – In this scenario PhenoMeNal is installed and run on servers managed and administrated by **EMBL-**EBI in datacentres selected by **EMBL-**EBI. The Hosting centre where **EMBL-**EBI's servers are located has their own GDPR and security procedures which control physical access. In this case, only non-identifiable anonymised data is permitted to be processed and therefore this processing is outside of GDPRs sensitive data definition.

EMBL-EBI only ever holds valid contact details (name, role, email address, telephone contact numbers) of these identified users in a password protected, secure access ERP system. This is governed by separate EMBL-EBI GDPR privacy notices.

The PhenoMeNal team have a documented process for these details to be added, amended and deleted on written request.

- **These obligations will relate to general principles such as:**

· Fulfilling data subjects rights with respect to their data.

· The accuracy of the data

· Data minimisation

· Limitation of purpose

· Transparency & fairness

· Lawfulness

Phenomenal has a number of tools and configuration options which can be utilised to further protect personal data against unauthorised or unlawful processing. These tools include:

Access Profiles
· These can be used to restrict the options available to administrators relating to user data.

Password Control
· The software can enforce password expiry, minimum length and format to improve overall system security.

Recommended Next Steps before you use Phenomenal:

- Know your obligations under GDPR
- Review all data for use in PhenoMeNal applications
- Anonymise and de-identify data for use in the Phenomenal open/cloud environment
- Assess current controls for access to and access within PhenoMeNal (do they need review and tightening?)
- Document processes to view, add, amend or delete such data
- Assess current process for providing personal details necessary for Phenomenal access
- Ensure that a documented internal process is present to request to view, add, amend or delete personal details.
- Take advice