HELMHOLTZ
MUNICH

Data Processing Agreement pursuant to Art. 28 GDPR

between

the User of the Helmholtz Munich Imputation Server
(hereinafter referred to as “Controller”)

and

Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt (GmbH), Ingolstädter Landstr. 1, D-85764 Neuherberg, Germany
(hereinafter referred to as “Processor”)

1. Subject matter of this agreement

1.1 The Controller uses the genotype imputation and phasing service provided by the Processor (Helmholtz Munich Imputation Server). The service is aimed at researchers wanting to impute many thousands of GWAS samples against a consistent reference in a consistent manner. This agreement (hereinafter referred to as “**Data Processing Agreement**”) adds provisions on processing on behalf of a controller pursuant to Article 28 GDPR to the Terms of Service agreed between the Controller and the Processor.

1.2 If the Processor, as part of his imputation service processes personal data (hereinafter referred to as “**Data**”) that he receives from the Controller the processing shall, without exception, be undertaken on behalf of the Controller and in accordance with the data processing rules set forth in Article 28 GDPR.

1.3 The Controller continues therefore, under data protection rules, to be the controller, i.e. the “Master of Data” and shall, with regard to the data subject, be responsible for evaluating the admissibility of data processing and safeguarding the rights of the data subjects.

1.4 This Agreement stipulates the details of data processing pursuant to Article 28 and 29 GDPR and takes priority over all other regulations agreed between the parties (hereinafter referred to as “**Parties**”) as far as the processing of Data by the Processor is concerned.

2. Details on data processing by the Processor on behalf of the Controller

2.1 The Processor offers a genotype imputation and phasing service where the Controller can upload GWAS data in VCF format on the imputation server of the Processor and receive imputed and phased genomes back**.** In this context, Data (genetic data), originating from patients/participants in clinical trials, uploaded by the Controller, are subject to the service offered by the Processor. The uploaded Data will be processed at the Processor's premises in Neuherberg and automatically deleted from the servers after 7 days.

On the Controller's side, it is the user of the services, i.e. the one who registers and uploads the data, who can give instructions to the Processor. On the part of the Processor, the recipients of instructions are those employees who are directly responsible for the support of the server.

2.2 The Processor shall process the data exclusively for the purposes specified in section 2.1; deviations are not permitted.

The Processor may process the Data in other ways only if, according to laws of the EU or the EU member state that he is subject to, he is legally obliged to do so; in such a case the Processor shall notify the Controller in writing of these legal requirements prior to processing unless the law in question forbids such notifications due to an important public interest. With the exception of the aforementioned legal obligations the Processor must not use the Data for other and, in particular, his own purposes and must not produce any copies or duplicates thereof.

2.3 The Processor may rectify or erase the Data or restrict the processing of Data only if instructed to do so by the Controller or if it is part of his services under section 2.1. In order to erase Data,

the Processor must use safe, state-of-the-art methods for which he must provide proof to the Controller upon his request.

2.4. If the data subject were to turn directly to the Processor to obtain information under data protection laws or due to other rights that the data subject is entitled to, the Processor must inform the Controller directly and await his specific instructions prior to any further action and communication.

2.5. The Processor warrants to strictly limit access to the Data to those persons who need to access the Data in order to render the agreed services. The Processor furthermore warrants to familiarise the persons engaged in performing the tasks, prior to their commencing the work, with the relevant data protection regulations and to ensure that they, while carrying out their work as well as thereafter, keep any information confidential and to oblige them to refrain from processing the data without due authorisation. To prove execution of this duty, the Processor shall send the Controller, following his request, the corresponding evidence, in particular copies of the declarations of obligation.

2.6 The Processor regularly controls and documents his own correct processing of the Data and compliance with the privacy regulations by the respective employees as well as the fulfilment of the duties under this Data Processing Agreement. Upon the request of the Controller, the Processor shall prove to him in writing all inspections undertaken by him and submit the corresponding documentation. The Processor shall furthermore ensure that all processing work performed by him under this Data Processing Agreement on behalf of the Controller is documented pursuant to Article 30(2) GDPR. At the request of the Controller, the Processor shall provide the Controller with the relevant documents.

2.7 The Processor shall notify the Controller forthwith and in writing, providing all the necessary details in the event of

(1) suspected violations of the protection of personal Data,

(2) breaches by him or his staff or third parties of data protection regulations or of stipulations included in the Contract,

(3) deviations of the technical and organisational measures of the Processor from the requirements agreed with the Controller,

(4) irregularities concerning the processing of Data,

(5) unauthorised access or unauthorised processing of Data and/or

(6) enquiries, inspection measures, investigations or other measures by a supervisory authority for data protection or another authority (e.g. police or court) directed at the Processor.

The Processor must, at the very latest, inform the Controller within 24 hours of becoming aware of a violation, deviation or irregularity.

The aforementioned notification duties shall also apply above all to any potential reporting and notification duties of the Controller pursuant to Articles 33 and 34 GDPR. The Processor warrants to duly assist the Controller with the performance of his duties pursuant to Articles 33 and 34 GDPR by, for example, providing the Controller with expert staff, making available relevant documents and answering his questions.

The Processor must not undertake, on behalf of the Controller, notifications according to Articles 33 and 34 GDPR unless he has been expressly instructed by the Controller to do so.

2.8 Notifications by the Processor according to section 2.8. above contain

(1) a description of the type of violation, deviation or irregularity, which must, as far as possible, be accompanied by an indication of the categories and an approximate number of the affected persons, the affected categories and an approximate number of the affected data sets;

(2) a description of the likely consequences of the violation, deviation or irregularity; and

(3) a description of the measures taken or suggested by the Processor in order to stop the violation, deviation or irregularity and, wherever necessary, a description of the measures to mitigate their potential adverse effects.

2.9 The Data Protection Officer of the Processor can be contacted under: Datenschutzbeauftragter des Helmholtz Zentrum München, Ingolstädter Landstr. 1, D-85764 Neuherberg, Germany, e-mail: datenschutz@helmholtz-muenchen.de

2.10 As far as the Data are concerned, the Processor shall assist the Controller with the appropriate technical and organisational measures to ensure that the rights of the data subject set forth in Articles 12 to 23 GDPR are upheld and to warrant compliance with the obligations of the Controller listed in Articles 32 to 36 GDPR regarding the security of personal Data, the potentially necessary assessment of consequences resulting from the privacy rules and any prior consultations with the supervisory authorities. The Processor must furthermore provide the Controller, at the Controller's request, with all information and details required by the Controller to meet other legal requirements affecting him (i.e. in order to draw up the list of processing activities).

2.11 The Processor warrants that the Data from other databases (the Processor's own or those of other customers of the Processor) are strictly separated.

3. Place of data processing by the Processor

3.1 The Processor processes the Data only in a member state of the European Union (EU) or in another country that has signed the Treaty on the European Economic Area (EEA); what matters is the status of the country at the time of processing. This also applies to simply accessing the data from such countries.

3.2 The Data may only be processed by the Processor at its registered office and its business branches. Access to the Data from outside (e.g. in the case of teleworking, home office, mobile working or similar) is only permitted if the Processor ensures through suitable technical and organisational measures that the level of data protection and data security is not impaired; this may include, for example, VPN connections and the exclusive use of terminal devices which the Processor has made available to its employees.

4. Engagement of sub-processors

The Processor will not use any sub-processors to perform the services agreed. The services shall be provided exclusively on the Processor's server environment, to which only employees of the Processor have access.

5. Technical and organisational security measures undertaken by the Processor

5.1 The Processor must ensure the security of processing pursuant to Article 32 GDPR especially in connection with Article 5(1)(2) GDPR. The Processor warrants therefore a level of security concerning the rendering of his services that is appropriate to the risk to the rights and freedoms enjoyed by the natural data subjects affected by the processing. To this end the Processor meets the security goals listed in Article 32 GDPR such as confidentiality, integrity and availability of the systems and services as well as their resilience regarding the type, scope, circumstances and purpose of the processing, by undertaking the appropriate technical and organisational measures, which, in the long run, exclude the risk as far as possible. An overview of the general technical and organisational measures taken by the Processor can be found here (https://imputationserver.helmholtz-munich.de/pdf/PR_TOMs_Public_v2.6_202308_engl.pdf).

5.2 The specific measures concerning the Helmholtz Munich Imputation Server are listed under Security - Helmholtz Munich Imputation Server (imputationserver-doc.readthedocs.io).
The Processor is obliged to maintain the measures during the term of this Data Processing Agreement. He shall furthermore observe the principles of due data processing.

5.3 For reasons of technical progress and development the Processor is permitted and, in the event of technical necessity, obliged to adjust individual measures as far as such measures are adequate and as far as the security level of the measures is not undercut. At the request of the

Controller, the Processor shall inform the Controller of such changes while material changes must be mutually agreed prior to their introduction.

6. Inspections by the Controller

6.1 The Processor agrees that the Controller may, at any time, monitor compliance with data protection regulations and with this Data Processing Agreement either himself or have it monitored by third parties by, in particular, obtaining information and viewing stored Data and data processing programs and undertake inspections, with an appropriate advance notice, on the premises of the Processor. The Controller is therefore obliged to treat all knowledge about business secrets and data protection measures of the Processor confidentially. This obligation shall remain even after termination of this Agreement.

6.2 The Processor warrants that he will, as far as necessary, join the Controller during his inspections, assist him and in particular allow him access and provide the relevant documents (records, reports of the Data Protection Officer, certifications, etc.).

7. Termination of data processing

7.1 Upon the request of the Controller, which may take place at any time, but at the latest upon termination of the data processing, the Processor must forthwith return to the Controller his Data in readable, commonly used, electronic format or physically erase it in line with data protection regulations if instructed to do so. This obligation does not apply if the Data has already been deleted due to the automatic deletion routines of the server.

7.2 Documentation produced by the Processor in order to prove that the Data has been processed duly and in line with contractual obligations as well as documents that are subject to the statutory safeguarding obligations of the Processor are excluded from the aforementioned rules to the extent necessary. It they contain Data the Processor must inform the Controller at the latest upon termination of the Data Processing Agreement.

8. Liability and mutual information

8.1 According to the statutory liability laws, the Processor shall be liable for any damage/loss caused to the Controller through the Processor's breaches of this Agreement and/or the statutory data protection rules applicable to him.

8.2 If, in connection with the data processing being performed hereunder, someone threatens or claims damages (Article 82 GDPR), fines (Article 83 GDPR) or other sanctions (Article 84 GDPR) against the Processor or the Controller, both must immediately inform one another thereof. Without prior agreement with the respective other party, the party concerned must not issue any statements or acknowledgements or declarations concerning a settlement; if the Processor and the Controller fail to come to an agreement as to how to defend themselves against such claims, the Controller as "Master of the Data" shall ultimately have the right to make the decision. In addition, both Parties must support each other in the defence of any claims made against them.

9. Miscellaneous

9.1 The Controller may cancel this Data Processing Agreement as well as the services agreed in the Terms of Service, at any time without notice, if the Processor commits a severe breach of the data protection regulations or the provisions set forth hereunder, if, despite reminders, he fails to execute an instruction of the Controller to be observed hereunder or if he, contrary to what has been agreed hereunder, refuses to allow the Controller to exercise his rights of inspection.

9.2. The right to retention according to Section 273 of the German Code of Civil Law [BGB] to the Data, parts thereof and data carriers of the Controller shall be excluded.

9.3 If the Data held by the Processor are threatened by confiscation or pledging, by insolvency proceedings or other events or measures of third parties, the Processor shall inform the

Controller forthwith. The Processor must inform all parties involved that the Controller is exclusively responsible and “Master of the Data”.

9.4 Changes or additions to this Data Processing Agreement or its parts and Appendices – including any assurances that may be made by the Processor – must be made in writing and require explicit reference to the fact that this is a change or addition to this Agreement. This also applies to a waiver of this written-form agreement. Written form in the aforementioned sense means the form set forth in Section 126 of the German Code of Civil law [BGB].

9.5 Statutory rules pursuant to this Data Processing Agreement also include the regulations issued by the EU.

9.6 Apart from section 9.4 hereunder, the use of the text form (i.e. e-mail) is deemed to be compliant with the written-form requirement pursuant to this Data Processing Agreement.

9.7 This Data Processing Agreement is governed by the law of the Federal Republic of Germany unless the GDPR contains provisions that take priority.

9.8 If some parts of this Data Processing Agreement were to be invalid, the validity of the remainder of this Data Processing Agreement shall not be affected thereby.