Data Processing Agreement

Parties	
Controller	**Processor**
You	Infermedica Sp. z. o. o (Plac Solny 14/350-062 Wroclaw, Poland) DPO - Marcin Kaleta phone: +48 791 204 765 email: dpo@infermedica.com
Definitions	
"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as updated from time to time; and "**Main Contract**" means a contract or agreement specifying the provision of services to the Controller; and "**System**" means a software provided by the Processor to the Controller in accordance with the Main Contract; and The terms "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**" and "**Process/Processing/Processed**" have the same meaning as described in GDPR and shall be construed accordingly.	
Subject-matter	Processing personal data by the Processor within the meaning of Art. 4(2) GDPR when performing the Main Contract
Duration of the processing	Upon expiration or termination of the Main Contract and/or, unless the provisions of DPA impose obligations going beyond this.

Nature and purpose of the processing	The activities involving the processing of Data are specified in the Main Contract and are related i) to the performance of the services ordered by the Controller, ii) to cybersecurity, iii) to perform analytics and to enable machine learning.
Type of personal data	Interview input data provided by the end-users of the System, i.e. age, birth date, sex, weight, height, symptoms, conditions, risk factors; output the System presents to the end-user
Categories of data subject	End-users of the System

Other rights and obligations

1. Processor:
    a. processes the personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law to which the processor is subject;
    b. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
    c. takes all measures required pursuant to Art. 32 GDPR (the scope of the measures is defined in „Technical and Organizational Measures")
    d. taking into account the nature of the processing, assists the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights;
    e. assists the Controller in ensuring compliance with the obligations pursuant to art. 32 to 36 GDPR taking into account the nature of processing and the information available to the Processor.
2. For the purposes of this provision, sub-contractual relationships shall be defined as services which directly relate to the provision of the main service. This does not include ancillary services which Processor uses, e.g. as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers or other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. Processor is, however, obliged to conclude appropriate and legally compliant contractual agreements and implement control measures to ensure data protection and data security of the Controller's Data, even in the case of outsourced ancillary services shall not engage another processor without prior authorisation of the Controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. The list of the accepted subcontractors is set forth in „Subcontractors" below.
4. Outsourcing to further subcontractors or the change of the existing subcontractor shall be permissible, provided that:
    a. Processor notifies the Controller of such further outsourcing or change within a reasonable period of time in writing or in text form; and
    b. the Controller does not object to the planned outsourcing in writing or in text form; and
    c. the commissioning of the new subcontractor is based on a contract in accordance with Art. 28(2)-(4) GDPR.
5. An objection pursuant to section 4(b) must be submitted by the Controller within a period of one week after the notification has been given. If Processor is unable to provide the service owed in the Main Contract due to the objection or can only do so at an economically unreasonable expense, Processor is entitled to terminate this Agreement and the Main Contract for good cause. A further subcontracting by the subcontractors is permitted. Processor must ensure that these subcontractors comply with the requirements of Art. 28 GDPR.
6. Controller has the right to carry out examinations in consultation with the Processor or to have them carried out by external auditors to be named in individual cases. Processor is entitled to reject external auditors based on objective reasons (e.g., if the external auditor is a competitor). The Controller has the right to verify compliance with this Agreement by Processor in the business operations of Processor by spot checks, which must be announced at least four weeks in advance.
7. Processor is entitled to claim reasonable compensation for enabling the Controller to perform controls.
8. At the end of the processing services, at the controller's discretion, erase or return to it any personal data and erase any existing copies thereof, unless Union or Member State law requires the retention of personal data, except the use of non-personal data, anonymous data in accordance with sec. 9 below. For the purpose of executing this Agreement, Processor shall be entitled to carry out all technically necessary processing, e.g., back-up copies, reading of log files etc., provided that this is necessary, the processing does not lead to a change in the content of the Data and this is in the interest of the Controller.
9. The Parties additionally agree that:
    a. any anonymous statistical information generated by the Data Subject, including but not limited to cases reported by users;
    b. anonymized information regarding diagnoses of users;
    c. any feedback and recommendations provided by Controller or their respective employees, partners or contractors regarding clinical accuracy, possible enhancements of the design or translations of the Processor software may be used without limitation by Processor to improve the Processor software and its product offering, even after termination of this Agreement, and are explicitly excluded from the obligation of confidentiality.

10. In the event that, in connection with the data processing operations covered by this Agreement, a claim for damages pursuant to Art. 82 GDPR, fines pursuant to Art. 83 GDPR and/or other sanctions pursuant to Art. 84 GDPR are threatened or asserted against one Party, this Party shall inform the other Party thereof immediately in writing. The Parties are obliged to support each other in the defense against such claims.

11. The Controller and Processor are liable for any damage resulting from data processing in accordance with Art. 82 GDPR to third parties.

12. In the internal relationship, the Parties shall have unlimited liability (i) in the event of intent, (ii) for damages resulting from injury to life, body or health and (iii) in the event that liability cannot be restricted pursuant to the applicable laws. In all other cases, Processor shall be liable only in the event of a breach of an "essential" obligation of the contractual relationship within the liability cap as determined in the Main Contract.

13. Polish law shall apply. Place of jurisdiction is the domicile of the Processor.

14. The provisions of this Agreement shall take precedence over any conflicting or deviating provisions from other existing contracts between the Parties.

15. Should any provision of this Agreement and/or its amendments or supplements be invalid, the validity of the remaining provisions shall not be affected. In the event of an invalid provision, the Parties shall be obliged to negotiate a valid and reasonable replacement provision which comes as close as possible to the purpose pursued by the Parties with the invalid provision.

Technical and Organizational Measures

Organizational measures

1. Access to paper documents is granted to authorized persons (CEO, Operations Director, Accountant, Legal, HR, CFO) such documents may also be made available to other personnel members on *need to know* basis, i.e. if it is necessary to perform their official or contractual duties.
2. Access to electronic documents is granted to authorized persons (CEO, Operations Director, Accountant, Legal, HR, CFO) with respect to the data of personnel members, and with respect to the data of clients and suppliers, such documents may also be made available to other personnel members *on a need to know basis*, i.e. if it is necessary to perform their official or contractual duties.
3. Selection of service providers, usage of verified or recommended providers with whom appropriate DPAs are concluded.
4. Use of cloud solutions that secure the complete loss of data which is maintained in paper form.
5. “Least privilege access policy” in place in terms of setting the user accounts.

Physical protection measures

1. Authorized access to offices as well as to every office room where personal data is processed. Cards are recorded, in the event of loss, actions are taken immediately to find it and ultimately to block the card.
2. Files containing personal data (employee documents, contracts with co-workers, contractors, customers) are stored in separate, locked cabinets.
3. Alarm system, security, monitoring in the building where the office is located.
4. Computers used by the personnel are protected by individual passwords, and the records of computers and systems installed are monitored by authorized persons from

the IT department.

Technical measures

1. Assigning and authenticating passwords to personnel accounts in electronic tools used by Infermedica (2-step verification).
2. Differentiated access to specific accounts on "*need to know basis*" (limited access to password managers, administrative accounts, access to databases in the cloud such as Dropbox). Access is granted to the functions that are responsible for a given area.
3. Means of automatically anonymizing data, such as shortening the IP address by the last digits so that it cannot be reproduced, and the place of origin identified.
4. Access to the WIFI network is separate for visitors and for the staff.
5. Back-ups shall be made at intervals of, as a general rule, 3 days and in some cases daily Back-ups are stored encrypted in an AWS S3 bucket (Standard-Infrequent Access - Designed for durability of 99.999999999% of objects across multiple Availability Zones).
6. Firewall rules allowing only necessary traffic inside our infrastructure.
7. Regular penetration testing.
8. Encryption at rest and in transit.
9. Employee disk encryption.
10. Google Cloud Armor as a DDoS protection and Web application firewall.
11. Multiple cloud compute zones used for high availability and reliability.

Subcontractors

The Controller agrees to the commissioning of the following Subcontractors under the condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR.

Company Subcontractor

Google Cloud Platform – hosting (Google Ireland Limited, with offices at Gordon House, Barrow Street, Dublin 4, Ireland)

*Amplitude- statistics (Amplitude, with offices at Inc., 501 2nd Street, Suite 100, San Francisco, CA 94107)

*Google Analytics- statistics (Google LLC, with offices at 1600 Amphitheatre Parkway Mountain View, California 94043)

Google Data Studio- statistics (Google Ireland Limited, with offices at Gordon House, Barrow Street, Dublin 4, Ireland)

Google Workspace – mail services (Google LLC, with offices at 1600 Amphitheatre Parkway Mountain View, California 94043)

Freshdesk – support service (Freshworks, Inc., with offices at 2950 S. Delaware Street, Suite 201, San Mateo, CA 94403)

OVH Sp. z o.o. – hosting services (OVH Sp. z o.o., with offices at ulica Swobodna 1, 50-088 Wrocław, Poland)

Amazon Web Services - hosting (Amazon Web Services Inc., with offices at 410 Terry Avenue North, Seattle, WA 98109-5210)

*If applicable