GUIDANCE FOR USE OF THIS DOCUMENT

To comply with the EU General Data Protection Regulations (GDPR), UK GDPR, and UK Data Protection Act 2018, Cumulus Neuroscience Ltd (Cumulus) have published this guidance on our privacy policy, which we follow where the Cumulus platform is being used to access, store and process personal data.

What is GDPR?

GDPR requires businesses to protect the personal data of European Union (EU) citizens and respecting individual data rights is a core value at Cumulus. As a company that may act as a data controller or data processor of personal data, GDPR applies to Cumulus.

How do we comply with the principles of GDPR?

GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Please note that we will retain personal data only for as long as necessary for the purposes for which it was collected; as required by law or regulatory guidance to which we are subject; and for the exercise or defence of legal claims that may be brought by or against us. Where Cumulus act as sponsor and data controller for a study, identifiable information about you will be retained for as long as is necessary for the purpose for which it is collected

All personally identifiable information that is collected by us is considered necessary to complete our research goals, where possible we collect the minimum amount of information required (data minimisation). All personal data is transmitted in an encrypted format, and stored on a secure database, where access is controlled. All participants have the right to remove their personal data from Cumulus systems, up until the point where it has been aggregated into group results. All

reasonable steps (data monitoring, automated data entry) will be taken to ensure personal data is accurate. Pseudoanonymisation is used to separate data collected using the Cumulus system from demographic data. All Cumulus data is keyed against a user ID number, meaning that in order to link personal demographic data with brain activity and behavioural data, a secured linking file must be used. Full anonymisation will be done as far as possible and at the earliest opportunity. Our research does not carry any decision decision-making related to individual data subjects, except in medical research that has been approved by a University research ethics committee, an NHS ethics committee, a UKRI-appointed ethics committee, or another research ethics committee.

We may share your personal data within the Group. This will involve transferring your data between the UK and the European Economic Area (EEA).

Whenever we transfer your personal data out of the UK or out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

a) We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.
b) Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

Disclosure of your information

We may disclose personal data to:

- third parties, including cloud service providers, who provide a service to us
- a public authority in the event that we are required to do so by law
- a third party where we are under a legal obligation to transfer it to that third party
- a prospective seller or buyer of any of our assets or business
- a third party where it is necessary to protect the vital interests of the data subject or another natural person

To the limited extent that it is necessary to transfer personal data outside of the EEA, we will ensure appropriate safeguards are in place to protect the privacy and integrity of such personal data, including standard contractual clauses under Article 46.2 of the GDPR. Please contact us if you wish to obtain information concerning such safeguards

Lawful Basis of Consent

Regarding consent, this is our primary basis for seeking participation in research. If participants agree to participate, the processing of their data may also be carried out under other lawful bases (legitimate interests).

Individuals give clear consent for us (and any relevant third-party data controller/processor) to process their personal data for a specific purpose: in our case this is in the context of research into brain health and cognitive performance.

We use information sheets and consent forms, which are regularly updated and reviewed. They use clear, simple language to specify why we want the data and what we will do with it (see language in Appendix 1 for example text to be included). Consent must be positively ‘opted-in’. Instructions are clearly given to ensure individuals know how to withdraw consent at any stage

without any negative consequences. Consents (hard copy) are stored by Cumulus in a secure, accesscontrolled filing cabinet.

Lawful Basis of Legitimate Interests
Given Cumulus's goal of understanding brain activity, there may be instances where data is processed under the lawful basis of legitimate interest.

With the aim of being fully transparent, we acknowledge that the data obtained may have additional value beyond that which is defined by the research study objectives and which may have an impact on health and social care. As a digital health company, we have a legitimate interest in using information relating to health, brain activity and behaviour for research studies. Therefore, we may use the data, collected through a research study, for additional research purposes beyond those outlined in the initial reason for collection, subject to GDPR requirements of safeguarding, transparency and fairness. This is to be made clear to participants and examples of the language to be used is in Appendix 1 below.

Data subject rights
We recognise and protect data subject rights as outlined in GDPR. In some cases, there are specific exemptions (subject to safeguards) to data subjects' rights if applying that right would prevent or seriously impair the achievement of the research purpose, research integrity and reproducibility, other legal requirements, resource implications and the impact on scientific validity.

Through the content provided on our information sheets, all data subjects are informed prior to data collection. Information sheets are designed to be concise, transparent, understandable and easily accessible.

We recognise the right of individuals to access a copy of their personal data, within 1 month of making a request. All requests will be recorded. Access to data does not include access to results of research or statistics at group level, nor in cases where the results are anonymised, nor where disclosure of data to the subject is deemed to have potential to cause distress (for example, health research data which may be taken out of context or used to infer something about disease state).

Participants have the right to remove their personal data from our Cumulus servers, up until the point where the results have been aggregated into group level analyses. Erasing data when a database has been locked for analysis would seriously impair achievement of the purposes of a research activity. This also applies in the case of rectification requested by a participant, as the research is based on a snapshot of time therefore if a rectification request is made, these will be considered on a case-by-case basis. These exemptions are clearly outlined prior to consent being given.

To the extent that we are a controller of your personal data you may request access to, rectification, or erasure of your personal data, or restriction of processing or object to processing of your personal data, as well as the right to data portability. In each case, these rights are subject to restrictions as laid down by law. The following is a summary of your rights:

- The right of access enables you to receive a copy of your personal data
- The right to rectification enables you to correct any inaccurate or incomplete personal data we hold about you
- The right to erasure enables you to ask us to delete your personal data in certain circumstances

- The right to restrict processing enables you to ask us to halt the processing of your personal data in certain circumstances,
- The right to object enables you to object to us processing your personal data on the basis of our legitimate interests (or those of a third party),
- The right to data portability enables you to request us to transmit personal data that you have provided to us, to a third party without hindrance, or to give you a copy of it so that you can transmit it to a third party, where technically feasible.

If you wish to make a complaint on how we have handled your personal data, you can contact our Data Protection Officer, Brian Murphy, who will investigate the matter (see contact details below). If you are unsatisfied with our response or believe we are processing your personal data in a way that is not lawful, you can complain to the Data Protection Commission (Ireland) or the Information Commissioner's Office (UK).

Regarding data subject rights in relation to automated individual decision making and profiling, this is relevant to us as a company. In our research using machine learning to classify individuals, participants give their explicit consent for their data to be used in this way.

We have notified the Irish Data Protection Commission of our DPO and are registered with the UK's Information Commissioner's Office (registration number ZA359889). Our Data Protection Officer is:

Brian Murphy
Email: dpo@cumulusneuro.com
Address: The CHQ Building, Custom House Quay, North Dock, Dublin 1

.

Appendix 1: Example Participant Information Sheet

General Data Protection Regulation (GDPR)
Participant Information

The EU General Data Protection Regulation (GDPR), along with the new UK Data Protection Act, will govern the processing (holding or use) of personal data for this study.

You are receiving this as you are currently a participant on this clinical research study. The information below details what data is held about you and who holds or stores this.

CUMULUS AS SPONSOR AND DATA CONTROLLER:

Cumulus are the sponsor for this study, based in the United Kingdom. The sponsor will use personal information from you and/or your medical records in order to undertake this study and will act as the **data controller** for this study. They are responsible for looking after your information and using it properly. Cumulus will keep identifiable information about you for 10 years after the study has finished, or for longer if that is required by the our legitimate purposes or the purposes of the project.

Cumulus use personally-identifiable information in order to conduct research to improve healthcare. As a digital health company, we have a legitimate interest in using information relating to your health and care for research, when you agree to take part in a research study. This means we will use your data, collected in the course of a research study, in the ways needed to conduct and analyse the research study.

WITHDRAWAL STATEMENT: Your rights to access, change or move your information are limited, as we need to manage your information in specific ways in order for the research to be reliable and accurate. If you withdraw from the study, we may have to keep certain information about you that we have already obtained however, where possible, we will remove your data from our system, up until the point of aggregation. To safeguard your rights, we will use the minimum personally-identifiable information possible.

COMPLAINT STATEMENT: If you wish to make a complaint on how we have handled your personal data, you can contact our Data Protection Officer, Brian Murphy, who will investigate the matter. If you are unsatisfied with our response or believe we are processing your personal data in a way that is not lawful, you can complain to the Data Protection Commission (Ireland) or the Information Commissioner's Office (UK).

USE OF DATA FROM THIS STUDY IN FUTURE RESEARCH:

When you agree to take part in a research study, the information about your health and care may be provided to researchers running other research studies in this organisation and in other

organisations. These organisations may be universities, NHS organisations or companies involved in health and care research in this country or abroad.

This information will not identify you and will not be combined with other information in a way that could identify you. The information will only be used for the purpose of health and care research and cannot be used to contact you or to affect your care. It will not be used to make decisions about future services available to you, such as insurance.