GDPR Data Protection Policy

Introduction

Cerebral Security Solutions Ltd hereafter referred to as Cerebral or we, takes its responsibilities with regard to the General Data Protection Regulation (GDPR) very seriously. This policy sets out how Cerebral manages those responsibilities, and to ensure all staff (including temporary and contractors) and visitors are aware of their responsibilities.

1. **Policy Statement**

Cerebral needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers, and clients and includes (but is not limited to), name, address, email address, date of birth, identification numbers, private and confidential information, sensitive information and bank details and categorised personal data. In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or statutory bodies. However, we are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), UK data protection laws and any other relevant data protection laws and codes of conduct. The company has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal data is one of our top priorities.

2. **Purpose**

The purpose of this policy is to ensure that Cerebral meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individual's, best interest.

The data protection laws include provisions that promote accountability and governance and as such the company has put comprehensive and effective measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches, ensuring good practice across Cerebral and uphold the protection of personal data.

3. **Scope**

This policy applies to anyone who has access to personal data as part of their relationship with Cerebral, and the company as a whole. This includes but is not limited to all staff and contractors that are permanent, fixed term, and temporary staff, any third-party representatives or sub- contractors, agency workers, volunteers, interns. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action, or in the case of non-employees e.g. sub-contractors, termination of contract may apply.

4. **Definitions**.

- **Data Controller** - means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, Cerebral is the data controller of all personal data relating to staff, customers and business contacts used in our business for our commercial purposes.
- **Data processor** - means a natural or legal person or organisation which processes personal data on behalf of a data controller. For the purposes of this Policy, cerebral is NOT a data processor.

- **Data subject** - means a living, identified, or identifiable natural person about whom Cerebral holds personal data.

- **Personal data** - means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject.
- **Personal data breach** - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed by or on behalf of Cerebral.
- **Special category personal data** - Special category data is personal data which the GDPR says is more sensitive, and so needs more protection e.g. medical data, criminal record etc.

5 General Data Protection Regulation (GDPR)

The ***General Data Protection Regulation (GDPR) (EU)2016/679)*** was approved by the European Commission in April 2016 and applies to all EU Member States from 25th May 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.
As cerebral processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

5.1 Personal Data

Information protected under the GDPR is known as "personal data"
Cerebral ensures that a high level of care is afforded to personal data falling within the GDPR's **'special categories'** (previously **sensitive personal data**), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.
In relation to the 'Special categories of Personal Data' the GDPR advises that:
"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Exemption clauses applies."

5.2 The GDPR Principles

Article 5 of the GDPR requires that personal data shall be:
a) processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency')**
b) 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, in accordance with Article 89(1), not be incompatible with the initial purposes **('purpose limitation')**
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation')**
d) 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 **('accuracy')**

e) 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject **('storage limitation')**
f) 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 **('integrity and confidentiality').**

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* **('accountability')** and requires that organisations such as cerebral show how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

6 Objectives

We are committed to ensuring that all personal data processed by and on behalf of cerebral is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.
Cerebral has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.
Cerebral will implement appropriate measures to ensure that:

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws.
- Every business practice, function and process carried out by the company, is monitored for compliance with the data protection laws and its principles.
- Personal data is only processed where we have verified and met the lawfulness of processing requirements.
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested.
- All employees are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their specific role.
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws.
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary.
- We monitor the Information Commissioner's Office, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements.
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection.
- We have appointed a Data Protection Officer who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR.
- We provide clear reporting lines and supervision with regards to data protection.
- We store and destroy all personal information, in accordance with GDPR regulations.

- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- Employees are aware of their own rights under the data protection laws.
- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements.

7 The Information Commissioners Office (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislations they have oversight for include: -

- The Data Protection Act 1998 (pre-25th May 2018)
- General Data Protection Regulation (post-25th May 2018)
- Data Protection Act 2018
- The Privacy and Electronic Communication (EU Directive) Regulations 2003
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004

The ICO's mission statement is “to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals” and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.
Under the data protection laws the ICO, as the UK's data protection authority (Supervisory Authority), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in the UK.
Cerebral is registered with ICO and appear on the Data Protection Register as a controller and/or processer of personal information.

8 Responsibilities

8.1 Data Protection Officer.

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on firms or Institutions to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform. Their role is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up to date with all legislation and changes relating to data protection.

The DPO will work in conjunction with senior management and Department Heads to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.
Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.

The data protection officer is responsible for administering this policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

8.2 Staff responsibilities

Staff members who process personal data or any other individual must comply with the requirements of this policy. Staff members must ensure that:

- all personal data is kept securely.
- no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.
- personal data is kept in accordance with Cerebral's screening and GDPR policy.
- any queries regarding data protection, including subject access requests and complaints, are promptly directed to the data protection officer.
- any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support them and the HR team in resolving breaches.
- where there is uncertainty around a data protection matter advice is sought from the Information Compliance team and the Data Protection Officer.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Data Protection Officer.

9 Website and internet

9.1 Personal Identifiable Information

Refers to any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains, including, but not limited to, name, address, phone number, fax number, email address, financial profiles, social security number, and credit card information. Personal Identifiable Information does not include information that is collected anonymously (that is, without identification of the individual user) or demographic information not connected to an identified individual.

9.2 What organisations are collecting the information.

In addition to our direct collection of information, our third-party service vendors (such as credit card companies, and banks) who may provide such services as credit, and insurance services may collect this information from our Visitors and Authorised Customers. We do not control how these third parties use such information, but we do ask them to disclose how they use personal information provided to them from Visitors and Authorised Customers. Some of these third parties may be intermediaries that act solely as links in the distribution chain, and do not store, retain, or use the information given to them.

9.3 How does the Site use Personally Identifiable Information

Cerebral uses Personally Identifiable Information to customise the Site, to make appropriate service offerings, and to fulfil buying and selling requests on the site. We may email Visitors and Authorised Customers about research or purchase and selling opportunities on the Site or information related to the subject matter of the Site. We may also use Personally Identifiable Information to contact Visitors and Authorised Customers in response to specific inquiries, or to provide requested information.

9.4 Who the information may be shared with.

Personal Identifiable Information about Authorised Customers may be shared with other Authorised Customers who wish to evaluate potential transactions with other Authorised Customers. We may share aggregated information about our Visitors, including the demographics of our Visitors and Authorized Customers, with our affiliated agencies and third-party vendors. We also offer the opportunity to "opt out" of receiving information or being contacted by us or by any agency acting on our behalf.

9.5 How is Personally Identifiable Information stored.

Personal Identifiable Information collected by Cerebral is securely stored and is not accessible to third parties or employees of Cerebral except for use as indicated above.

9.6 Cookies

Cookies are used for a variety of reasons. We use Cookies to obtain information about the preferences of our Visitors and the services they select. We also use Cookies for security purposes to protect our Authorised Customers. For example, if an Authorised Customer is logged on and the site is unused for more than 10 minutes, we will automatically log the Authorised Customer off.

9.7 How do we use login information

Cerebral Security Solutions Ltd uses login information, including, but not limited to, IP addresses, ISPs, and browser types, to analyse trends, administer the Site, track a user's movement and use, and gather broad demographic information.

9.10 What partners or service providers have access to Personal Identifiable Information from Visitors and/or Authorised Customers on the Site

Cerebral has entered and will continue to enter partnerships and other affiliations with several vendors. Such vendors may have access to certain Personally Identifiable Information on a need-to-know basis for evaluating Authorised Customers for service eligibility. Our privacy policy does not cover their collection or use of this information. We will disclose Personal Identifiable Information to comply with a court order or a request from a law enforcement agency to release information. We will also disclose Personal Identifiable Information when reasonably necessary to protect the safety of our Visitors and Authorised Customers.

9.11 How does the Site keep Personally Identifiable Information secure

All of our employees are familiar with our security policy and practices. The Personally Identifiable Information of our Visitors and Authorised Customers is only accessible to a limited number of qualified employees who are given a password in order to gain access to the information. We audit our security systems and processes on a regular basis. Sensitive information, such as credit card numbers or social security numbers, is protected by encryption protocols, in place to protect information sent over the Internet. While we take commercially reasonable measures to maintain a secure site, electronic communications and databases are subject to errors, tampering and break-ins, and we cannot guarantee or warrant that such events will not take place and we will not be liable to Visitors or Authorized Customers for any such occurrences.

10 Governance Procedures

10.1 Accountability & Compliance

The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines, and is responsible for, and be able to demonstrate compliance.

10.2 Purpose limitation & Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be 'limited to what is necessary', which forms the basis of our minimalist approach. We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary. Cerebral collects and processes the personal data directly from data subjects.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data

minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes:

- Electronic collection (i.e. forms, website, surveys etc.) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include 'optional' fields, as optional denotes that it is not necessary to obtain
- Forms, contact pages and any documents used to collect personal information are reviewed to ensure they are fit for purpose and only obtaining necessary personal information in relation to the legal basis being relied on and the purpose of processing.

10.3 Encryption
Cerebral utilise encryption as a further risk prevention measure for securing the personal data that we hold. Encryption via password protection is used for transferring personal data to any external party and provide the password in a separate format.

10.4 Restriction
we use restriction methods for all personal data activities. Restricting access is built into the foundation of the Cerebral processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information.

10.5 Hard Copy Data
Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (*i.e. copies of patient records, hospital invoices or claims information*). Where this is necessary, we aim to minimise the information we hold and/or the length of time we hold it for. **Steps include:**

- we will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (i.e. when the data is being passed to a third-party for processing and not directly to the data subject)
- Recipients (i.e. the data subject, third-party processer) are re-verified and their identity and contact details checked.
- The Data Protection Officer advises on the transfer.

If for any reason a copy of the paper data must be retained by Cerebral, it must be kept in a secured lockable filing cabinet in accordance with the British standards.

10.6 Legal basis for processing (lawfulness)

At the core of all personal information processing activities undertaken by cerebral, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where one of the following applies:

- the data subject has given consent to the processing of their personal data for one or more specific purposes.
- the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.

- the processing is necessary for compliance with a legal obligation to which the data controller is subject.
- the processing is necessary to protect the vital interests of the data subject or of another natural person.
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
- the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

If the personal data in question is special category personal data (also known as “sensitive personal data”), at least one of the following conditions must be met:

a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless relevant laws prohibit them from doing so).
b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by UK law or other applicable EU laws which provide for appropriate safeguards for the fundamental rights and interests of the data subject);
c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
d) the processing relates to personal data which is manifestly made public by the data subject.
e) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.
f) the processing is necessary for substantial public interest reasons, which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.
g) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR.

10.8 Third-Party Processors

Cerebral security utilises external processors for certain processing activities (where applicable). We keep records of all personal data that is processed outside of cerebral, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing includes (but is not limited to):

- Human Resources
- Hosting or Email Servers
- Direct Marketing/Mailing Services
- Security screening suppliers

We have strict due diligence, procedures and measures in place to review, assess and background check all processors prior to forming a business relationship, (preferred Supplier policy) We obtain cerebral documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

We audit their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

10.9 Data Retention & Erasure

Cerebral have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. Retention schedules will govern the period that records will be retained and can be found in the Record Retention Table. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritises the protection of the personal data in all instances.

10.9.1 Retention Period Protocols

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All Cerebral and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

10.9.2 For all data and records obtained, used and stored within Cerebral, we:

a. Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain.

b. Establish periodical reviews of data retained.

c. Establish and verify retention periods for the data, with special consideration given in the below areas:

(1) the requirements of Cerebral Security.
(2) the type of personal data.
(3) the purpose of processing.
(4) lawful basis for processing.
(5) the categories of data subjects.

d. Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, Cerebral will identify the criteria by which the period can be determined and provide this to the data subject on request.
e. Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered.

10.9.3 Records of Processing Activities

As an organisation with less than 250 employees cerebral only has to document our processing activities when they are:

- Not occasional; or
- Could result in a risk to the rights and freedoms of individuals; or
- Involve the processing of special categories of date or criminal conviction and offence data.

These are recorded in our (Information Asset Register) which is readily available to the Information Commissioner's Office upon request.

Acting in the capacity as a controller (or a representative), our internal records of the processing activities carried out under our responsibility, contain the following information:

- Our full name and contact details and the name and contact details of the Data Protection Officer. Where applicable, we also record any joint controller.
- The purposes of the processing
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has or will be disclosed (including any recipients in third countries or international organisations)
- Where possible, the envisaged time limits for erasure of the different categories of data
- A general description of the processing security measures.

As part of our obligations under the UK's Data Protection Act 2018, Sch.1, Pt.4, where we are required to maintain a record of our processing activities in our capacity as a controller and are processing special category or criminal conviction data, as specified in Sch.1, Pt.1-3 of the Act, we also record the below information on the register:

- Which condition is relied on?
- How the processing satisfies Article 6 of the data protection laws (lawfulness of processing)
- Whether the personal data is retained and erased.

10.9.4 Designated Owners

All systems and records have designated owners throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, business area and level of access to the data required. The designated owner is recorded on the Retention Register. Data and records should never be, removed, accessed or destroyed without the prior authorisation and knowledge of the designated owner.

10.9.5 Suspension of Record Disposal for Litigation or Claims

If Cerebral is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our company, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

10.9.6 Expiration of Retention Period

Once a record or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR requirements or to archive records for a further period.

10.9.7 Destruction and Disposal of Records & Data

All information on paper or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, and customers.

Cerebral is committed to the secure and safe disposal of any waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data

Protection Regulation (GDPR) and that employees are trained and advised accordingly on the procedures and controls in place.

10.9.8 Paper Records.
Due to the nature of our business, Cerebral retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. Cerebral use a shredder that complies with the ISO/IEC 21964 standard.

10.9.9 Electronic & IT Records and Systems
Cerebral uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active; this disposal is handled in an ethical and secure manner.
The deletion of electronic records will be done by the Director who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up to date a register of destroyed records.

10.9.10 Internal Correspondence and General Memoranda
Unless otherwise stated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support (i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed).
Where correspondence or memoranda that do not pertain to any documents having already been assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases or at a maximum of 2 years.

Examples of correspondence and routine memoranda include (but are not limited to):

- Internal emails.
- Meeting notes and agendas.
- General inquiries and replies.
- Letter, notes or emails of inconsequential subject matter.

10.9.11 Erasure
In specific circumstances, data subjects' have the right to request that their personal data is erased, however Cerebral recognise that this is not an absolute 'right to be forgotten'. Data subjects only have a right to have personal data erased.

10.9.12 Retention Periods
Cerebral security has a Retention register that outlines the retention periods and the subsequent actions upon reaching said dates. Where no defined or legal period exists for a record, the default standard retention period is 6 years plus the current year.

11 Data subject rights procedures

11.1 Consent &the right to be informed.
The collection of personal and sometimes special category data is fundamental In the safe running of cerebral. we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws. The data protection law defines consent as; 'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or

she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

Where processing is based on consent, Cerebral have reviewed and revised all consent mechanisms to ensure that:

- Consent requests are transparent, using plain language and using no illegible terms, jargon or extensive legal terms.
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes.
- Consent is always given by a statement or a clear affirmative action (positive opt-in) which signifies agreement to the processing of personal data.
- Consent mechanisms are upfront, clear, granular (in fine detail) and easy to use and understand.
- Pre-ticked, opt-in boxes are never used.
- Where consent is given as part of other matters (i.e. terms & conditions, agreements, contracts), we ensure that the consent is separate from the other matters.
- Along with Cerebral name, we also provide details of any other third party who will use or rely on the consent.
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case.
- If special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.
- For special category data, the consent obtained is explicit (stated clearly and in detail, leaving no room for confusion or doubt) with the processing purpose(s) always being specified.
- How we gain consent is assessed and reviewed regularly.

11.2 Consent Controls

Cerebral maintains rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances. Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and plain language.

11.3 Alternatives to Consent

Cerebral recognise that there are six lawful bases for processing and that consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor:

- Where we ask for consent but would still process it even if it was not given *(or withdrawn).* If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use.
- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate.
- Where there is an imbalance in the relationship, i.e. with employees

11.4 Information Provisions
Where personal data is obtained directly from the individual *(i.e. through consent, by employees etc.,* written materials and/or electronic formats (i.e. website forms, subscriptions*,* email, etc.), we provide the below information in all instances, **in the form of a privacy notice:**

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our data protection officer
- The purpose(s) of the processing for which the personal information is intended.
- The legal basis for the processing
- The recipients or categories of recipients of the personal data *(if applicable)*
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- The right to lodge a complaint with the Supervisory Authority.
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent unless there is a legal requirement to keep the information longer.

11.5 Privacy Notice
Cerebral defines a Privacy Notice as a document, form, webpage or pop-up that is provided to individuals at the time we collect their personal *data (or at the earliest possibility where that data is obtained indirectly)*. Our Privacy Notices includes the Article 13 (*where collected directly from individual*) or *14 (where not collected directly)* requirements and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

The notice is easily accessible, legible and jargon-free and is available in several formats, dependent on the method of data collection: -

- Via our website
- Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face.
- In employee contracts and recruitment materials
- Printed media, adverts and financial promotions

11.6 Employee Personal Data
Our HR procedures have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Terms and Conditions booklet which informs them of their rights under the data protection laws, how to exercise these rights and are provided with a Privacy Notice specific to the personal information we collect and process about them.

All employees have the ability to exercise their rights as a data subject.

11.7 The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided subject to a £10 administration fee, it is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*). Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

11.8 Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d), all data held and processed by Cerebral is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The responsible person is notified of the data subject's request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

12. Security & Breach Management

Cerebral ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred.

12.1 What Is A Personal Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (for example sending an email or SMS to the wrong recipient).
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

12.2 When we report a breach

Cerebral must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination.
- potential or actual financial loss.
- potential or actual loss of confidentiality.
- risk to physical safety or reputation.
- exposure to identity theft (for example through the release of non-public identifiers such as passport details).
- the exposure of the private aspect of a person's life becoming known by others. If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

12.3 Reporting A Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should Complete a data breach report form which can be obtained from the Office Manager, and Email the completed form to Info@cerebralsecurity.co.uk.

Where appropriate, you should liaise with your line manager about completion of the data report form. Breach reporting is encouraged throughout Cerebral and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, Office Manage or the DPO. Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The Appointed person will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

12.4 Managing and Recording The Breach

On being notified of a suspected personal data breach, The Relevant personnel if it is not the DPO, will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:

- Where possible, contain the data breach.
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed.
- Assess and record the breach in the School's data breach register.
- Notify the ICO.
- Notify data subjects affected by the breach.
- Notify other appropriate parties to the breach.

- Take steps to prevent future breaches.

12.5 Notifying the ICO
The relevant personnel will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals. This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. If they are unsure of whether to report a breach, the assumption will be to report it. Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

12.6 Notifying Data Subjects
Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, HR will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures Cerebral have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, The responsible personnel will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police). If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then Cerebral will consider alternative means to make those affected aware (for example by making a statement on Cerebral's website).

12.7 Notifying Other Authorities
Cerebral will need to consider whether other parties need to be notified of the breach. For example:

- Insurers.
- Third parties (for example when they are also affected by the breach).
- Local authority.
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

12.8 Assessing The Breach
Once initial reporting procedures have been carried out, Cerebral will carry out all necessary investigations into the breach. We will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data). Having dealt with containing the breach, Cerebral will consider the risks associated with the breach.
These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is.
- The volume of data affected.
- Who is affected by the breach (i.e. the categories and number of people involved).
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise.
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation).
- What has happened to the data.
- What could the data tell a third party about the data subject.
- What are the likely consequences of the personal data breach on Cerebral.
- Any other wider consequences which may be applicable.

12.9 Preventing Future Breaches

Once the data breach has been dealt with, Cerebral will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred.
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again.
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice.
- Consider whether its necessary to conduct a privacy or data protection impact assessment.
- Consider whether further audits or data protection steps need to be taken.
- To update the data breach register.

12.10 Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to Your line manager, Office Manager or the DPO. This can help capture risks as they emerge, protect Cerebral from data breaches and keep our processes up to date and effective

13. Transfers & Data Sharing

Cerebral takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is encrypted with a Password and where possible is also subject to our data minimisation methods.

We use approved, secure methods of transfer. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible.

14. Training

Through our strong commitment and robust controls, leaders ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role through our Performance Development Review process and regular 1 to 1s.

Our **Staff Training policy** details requirements relating to mandatory training, of which GDPR is included. Completion of mandatory training is a contractual requirement on all employees and adherence is monitored at a senior leadership level facilitated centrally by HR.

15 Complaints

15.1 Scope

Generally, data protection complaints can be grouped into one of four possible reasons:

• How their personal data has been processed
• How their 'Subject Access Request' has been handled
• How their complaint has been handled
• Appeal against a decision made following a complaint

Please see our **complaints policy and procedure** for more information.

15.2 Submitting a Complaint
If you wish to complain to Cerebral about how your personal information has been processed, or your GDPR complaint has been handled, or appeal against any decision made following a complaint, you can do so using our complaint form attached to our **complaints policy and procedure** or send it directly to Cerebral's Data Protection Officer via email.

Complaints should be submitted in writing and submitted to: info@cerebralsecurity.co.uk

Post: Thornton House, Bristol Road, Farrington Gurney, BS396TQ

The DPO will acknowledge receipt within 3 working days.

The Data Protection Officer will review and respond in writing, to your complaint within 28 working days of receipt of the complaint. If an extension is required, this will be with the agreement of both parties and up to a maximum of a further 10 working days.

If you are dissatisfied with the way in which your complaint has been handled or the outcome from your complaint, then you may write outlining your concerns to the DPO where an Independent member will review your concerns and respond within 28 working days.
If you remain dissatisfied, you may forward your complaint to:
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow Cheshire SK9 5AF or via https://ico.org.uk/make-a-complaint/.

16 Review

This policy may be subject to change; therefore all employees are required to sign to confirm that they have read and agree to abide by this policy each time it is revised.

This is to improve accountability of all staff, and to drive the continual improvement of our operation; thus, improving the effectiveness of our safety measures.

This policy is subject to annual review by HR and the Data protection officer, with changes made as required by legislation or set out by our internal review processes; Once reviewed it is then checked and signed off by the Managing Director of Cerebral.