GDPR Policy

ACCLAIM BIOMEDICAL CONSULTING Ltd.

1 POLICY STATEMENT

Acclaim Biomedical Consulting Ltd is fully committed to compliance with the requirements of the EU General Data Protection Regulation. The company will therefore aim to ensure that all employees, contractors, agents, consultants, or partners of the company who have access to any personal data held by or on behalf of the company, are fully aware of and abide by their duties and responsibilities under the Regulation.

2 PURPOSE

The company needs to collect and use certain types of information about people with whom it deals in order to perform its functions. This includes information on current, past and prospective suppliers, clients, customers, service users and others with whom it communicates. The company collects and uses certain types of information defined as fair use materials in order to deliver its contractual duties . This information must be dealt with properly whether it is collected, recorded and used on paper, computer, or other material. There are safeguards to ensure this in the EU General Data Protection Regulation.

The company regards the lawful and correct treatment of personal information as critical to successful operations, and to maintaining confidence between those with whom we deal and ourselves. It is essential that it treats personal information lawfully and correctly.

The purpose of this policy is to explain how the company will ensure compliance with the EU General Data Protection Regulation. It includes organisational measures and individual responsibilities which aim to ensure that the company complies with the Data Protection principles and respects the rights of individuals. This policy provides outline measures and puts in place a structure for monitoring compliance.

3 LEGAL CONTEXT AND DEFINITIONS

3.1 EU General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) governs how information about people (Personal Data) should be treated. It also gives rights to individuals whose data is held. The Regulation came into force on 25 May 2018 and applies to all personal data collected at any time whether held on computer or manual record. The Regulation is enforced by the Information Commissioner.

The GDPR makes a distinction between personal data and "sensitive" personal data. Sensitive personal data is subject to stricter conditions of processing.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or

indirectly, in particular by reference to an identifier such as a name, an 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 natural person.
Sensitive personal data is defined as personal data consisting of information as to:
Racial or ethnic origin; political opinions; religious or philosophical beliefs; or trade union membership; 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.

A Data Subject is an individual who is the subject of the data.

A Data Controller is an organisation, or person that determines the purposes for which and the manner in which any personal data is to be processed.

A Data processor is any organisation or person who processes data on behalf of the data controller.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The GDPR contains 6 principles for processing personal data with which organisations must comply.
Personal data shall be:

(1) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
(2) 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 considered to be incompatible with the initial purposes ('purpose limitation');
(3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
(4) 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');
(5) 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');
(6) 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').

Data subject rights are:

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information.
- The right to prevent processing in certain circumstances.
- The right to rectify, block or erase information which is regarded as wrong information.
- The right to have decisions reviewed where they have been made automatically.
- The right to object to receiving marketing information.

4 SCOPE

4.1 Context of this policy

This policy applies to all the staff, contractors and organisations that use personal data in support of their work on behalf of the company.

The policy should be read in conjunction with the Ethics and Anti-Corruption Policy governing the professional conduct and standards of staff.

4.2 Personal data held

This policy applies to all processing of personal data held by the company. This includes:

- Personal data processed by the company.
- Personal data controlled by the company but processed by another organisation, on the company's behalf (for example private sector contractors; and service level agreements with voluntary sector organisations).
- Personal data processed jointly by the company and its partners

Personal data held by the company may be held in many forms including:

- Database records;
- Computer files;
- Emails;
- Sound recordings;
- Photographs;
- Website;
- Mobile phones.

Data subjects may include:

- Current, past and prospective employees;
- Suppliers;
- Clients;
- Customers;
- Service users;
- Others with whom the company communicates.

5 RESPONSIBILITIES AND PENALTIES

5.1 Organisational Responsibilities

Acclaim Biomedical Consulting Ltd is a data controller under the EU General Data Protection Regulation.

5.2 Individual Responsibilities

Every employee must comply with this policy. Failure to comply with the policy may result in disciplinary action which could include dismissal.

All contractors/ service providers must comply with the policy when using personal data supplied to / held by the company to facilitate the commissioned service being provided.
It is a criminal offence to access personal data held by the company for other than company business, or to procure the disclosure of personal data to a third party.
It is a further offence to sell such data.

Employees who access or use personal data held by the company for their own purposes will be in breach of relevant policies of the company, including but not limited to the Code of Conduct and the Online Safety Policy, and subject to disciplinary action, which could include dismissal, and may also face criminal proceedings.

6 PURPOSES OF PROCESSING PERSONAL DATA AND FAIRNESS

The company will collect and process personal data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
The company will use a condition of processing as detailed in Article 6(1) of the GDPR of their personal data.

i. the data subject is being used for fair purposes for the commercial operations of the company;
ii. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
iii. processing is necessary for compliance with a legal obligation to which the controller is subject;
iv. processing is necessary for the performance of a task carried on behalf of the company vested in the controller;

When sensitive data is collected, the company will use a condition of processing as detailed in Article 9 of the GDPR. These include protecting the vital interests of the data subject or meeting a legal obligation.

In cases where consent is obtained, the consent must be free and informed and may be changed at any time.

Acclaim Biomedical do not hold personal details or information other than those provided by individuals and commercial organisations for the purposes of conducting the day to day business and communications of the company.

When personal data is to be used for a new purpose then the fairness information will be provided to the data subject again and if necessary a new consent will be sought.

People are free to ask for more details about how their personal data is being used at any time and if unhappy about how their data is used may make a complaint.

Any person whose details (including photographs) are to be included on the company's website will have been deemed to have provided consent along with the information provided. At the time the information is included or collected, all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

7 DATA QUALITY, INTEGRITY AND RETENTION

- Personal data held will be relevant to the stated purpose and adequate but not excessive.
- The company will ensure, as far as is practicable, that the information held is accurate and up-to-date.
- If personal data is found to be inaccurate, this will be remedied as soon as possible.
- Personal information, such as contact details, may be shared within the company where it is necessary to keep records accurate and up-to-date, and in order to provide individuals with a better service.
- Records may include professional opinions about individuals but employees will not record any personal opinions about individuals.
- Information will only be held for as long as is necessary after which the details will normally be deleted. Where details of individuals are stored for long-term archive or historical reasons, and where it is necessary to retain the personal detail within the records, it will be done within the requirements of the legislation.
- Redundant personal data will be destroyed using the company's procedure for disposal of confidential waste and in accordance with retention schedules.

8 SECURITY

- Any inappropriate, unauthorised access of data, use or misuse of data or failure to comply with ICT security arrangements and policies may result in disciplinary action, including dismissal.
- The company will implement appropriate technical and organisational security measures so that unauthorised staff and other individuals are prevented from gaining access to personal information.
- An employee must only access personal data they need to use as part of their job. Inappropriate or unauthorised access may result in disciplinary action, including dismissal and criminal prosecution.
- All data breaches (however minor) should be reported

.

- All staff within the company will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.
- Manual files and other records or documents containing personal/sensitive data will be kept in a secure environment and accessed on a need-to-know basis only.
- Personal data held on computers and computer systems will be installed with user-profile type password controls. Personal data should not be held on unencrypted electronic devices.
- Personal data will not be transferred outside the European Economic Area without the approval of the data controller.

9 DATA SUBJECTS RIGHTS

- The company will ensure that the rights of people about whom the information is held can be fully exercised under the Regulation.
- The company will provide individuals with a copy of the information held about them within one month of receiving a request (subject access). This period may be extended by two further months where necessary, taking into account the complexity and number of the requests.
- On receiving a request for subject access the company will check and require evidence of the identity of the individual and any further information required to isolate the records of that individual.
- Where a subject access request has a broad scope, the company may ask for more details from the data subject in order to locate the information that is of particular interest.
- Where a large volume of information is held, the company may seek to make the information available in ways other than providing a copy. This could include arranging an appointment for the data to be inspected within the company.
- The introduction of the right of access to non-personal information held by the company under the Freedom of Information Act 2000 may also need to be considered. This is because some requests may be for a combination of personal and non-personal information.
- The company will comply immediately with a request from an individual to cease sending them marketing or consultation information.
- Requests from individuals to correct, rectify, block, or erase information that they regard as wrong information or to stop processing that is causing damage or distress will be considered by the company on a case by case basis. The individual concerned will be fully informed of the resulting decision and the reasons for it. Legal advice will be sought by the company should a request not be supported, or if considered sensitive/complex before coming to a decision.
- An individual wishing to exercise any of their rights under the GDPR should put their request in writing to the company.
- All Subject Access requests received will be recorded for monitoring and reporting purposes.

AcclaimBiomedical
Consulting Ltd

10 DISCLOSURE AND SHARING

10.1 Third party access to information

Where a request for personal data is made by a third party on behalf of the data subject it shall be treated as a subject access request. Evidence is required that the third party is entitled to act in this way, such as a written statement from the data subject or an enduring power of attorney. Appropriate professionals may need to be consulted before a decision to release the personal data is made.

Occasionally third party information may form part of the data extracted in response to a subject access request. In deciding whether to release this information, the company will consider the following:

- any duty of confidentiality owed to the third party;
- attempts to get consent from the third party;
- any express refusal of consent from the third party;
- the third party's expectations with respect to that data.

When a request for personal data is made by a third party and not on behalf of the data subject, the company shall consider the request under Freedom of Information as well as GDPR. It shall consider whether releasing the personal data would breach any of the Data Protection principles and in particular whether any exemptions under GDPR apply. Personal information will not be shared with third parties unless specifically allowed for in law and justified in the specific situation.

When there is a specific reason for requesting the information, an exemption under GDPR may apply. Examples are where information is required for the prevention or detection of crime, apprehension or prosecution of offenders or assessment or collection of tax.

If an appropriate exemption under GDPR does apply so that the Data Protection principles will not be breached, the company will usually comply with the request. However, without a Court Order there is no obligation on the company to disclose the information.
Where the company is not convinced that the third party has entitlement to the personal data, or that any exemptions under GDPR apply, and that releasing information would breach the Data Protection principles, the personal data will be withheld and only released on presentation of a Court Order.

10.2 Information sharing

The company promotes information sharing where it is in the best interests of the data subject. However, personal sensitive data will not be shared unless it is in connection with the primary purpose for which the information was collected, or the data subject has explicitly given their permission for the information to be shared for this purpose, or another legal provision (GDPR exemption exists) to allow the sharing such information.
The company will ensure that supporting processes and documentation are made available to professionals so that they understand how to share information safely and lawfully.
Where an employee acting in good faith has shared information in accordance with these supporting processes and documentation, they shall not normally be subject to disciplinary action under section 5.2, hereof.

Sharing large sets of information, or recurrent regular sharing shall be carried out under written agreement to ensure the continued compliance with the GDPR and that additional safeguards can be considered and put in place.

10.3 Contractual and partnership arrangements

When the company enters contractual or partnership arrangements which involve the processing of personal data, a written agreement will specify which party is data controller or whether there are joint data controller arrangements. Where a third party is processing personal data and information on behalf of the company, a written contract will be put in place. Specific care will be taken in respect of services provided online and via 'the cloud'.

Where the company remains as data controller, it will take steps to ensure that the processing by its contractors and sub-contractors will comply with GDPR. Contractors will not be able to sub-contract Data Processing without the explicit written permission of the company. Staff will take reasonable steps to ensure that data processing by third parties is regularly monitored to ensure GDPR requirements are being met.

Where the parties are data controllers jointly or in common, the company will liaise with the other party to ensure that all processing complies with GDPR. The responsibilities of each data controller should be expressly and clearly laid out.

All contractors who are users of personal information supplied by the company will be required to confirm that they will abide by the requirements of the Regulation to the same standard as the company with regard to information supplied by the company. Staff should obtain advice from Legal Services as necessary.

All contractors, consultants, partners or agents of the company must ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the company, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Regulation. Any breach of any provision of the Regulation will be deemed as being a breach of the contract between the company and that individual, company, partner or firm. The company shall take reasonable steps to ensure regular monitoring of contracts and specifically the security of data being processed on its behalf.
Any observed or suspected security incidents or security concerns should be reported to the company.

All contractors, consultants, partners or agents of the company must allow data protection audits by the company of data held on its behalf if requested in line with these contractual arrangements.

All contractors, consultants, partners or agents of the company must indemnify the company against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

AcclaimBiomedical
Consulting Ltd

11 NOTIFICATION

The company has assessed its obligations using the ICO website and determined that there is no current obligation for the company to register with the Information Commissioners Office based on the type and scope of data processing conducted.

12 SUBJECT ACCESS REQUESTS AND DATA PROTECTION COMPLAINTS

Subject access requests and data protection complaints should be addressed to:

- Managing Director, Acclaim Biomedical Consulting Ltd, 20 Sandford Leaze, Avening, Gloucestershire, GL8 8PB. info@acclaimbiomedical.co.uk

Complaints about the company's processing of personal data and rights under the General Data Protection Regulation will be dealt with in accordance with this Policy. Complaints will be fully dealt with after a formal review.

Individuals have a right to request that the Information Commissioner make an assessment of compliance of particular circumstances with the General Data Protection Regulation. If individuals are not happy about how we have handled their information they can contact the ICO via the following means:
sent to

Customer Contact
Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

Alternatively visit their website - www.ico.gov.uk or contact them by phone on 03031231113
The company will respond promptly and fully to any request for information about data protection compliance made by the Information Commissioner.
The company will comply with any Information Commissioner Information Notice (to provide answers and information to the Commissioner) or Enforcement Notice (for failure to provide answers or information or for a breach of the Act) sent to the company by the Information Commissioner. The Commissioner can also carry out audits, prosecute individuals and organisations and report concerns to parliament.

AcclaimBiomedical
Consulting Ltd

14 IMPLEMENTATION

The responsibility for implementation of this policy rests with the company.
The company will ensure that:

- Everyone managing and/or handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and/or handling personal information is appropriately trained to do so.
- Everyone managing and/or handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, is given advice as necessary.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- Employees are aware of the action required in the event of a Data Breach.

On joining the company, employees are required to undertake training on Data Protection and Security as part of their induction. They will not be allowed to use the company's network until successfully completing the training.

The Data Protection Officer works with the company to maintain the on-going programme of annual training and awareness to maintain a high level of understanding of Data Protection and security among all staff and to communicate any legal or policy changes that occur.

Supporting procedures for this policy maybe created and are maintained .

Data Protection audits are regularly carried out by internal audit (external audits may be commissioned if required) in order to monitor compliance with the GDPR and this policy.
The governing body will receive an annual report on data governance generally; this will also include details of any data breaches.

15 Monitoring and Review

This policy will be reviewed at not more than 2-yearly intervals.

Acclaim Biomedical Consulting Ltd will always aim to meet the highest standards of ethical conduct in all aspects of the company's operation. To this end, the company has aligned it activities with the Business Code of Conduct published by the ABHI (association of British Healthcare Industries, http://www.abhicodeofpractice.org.uk/cobp-documents.aspx)

For	Signed	Date
Acclaim Biomedical Consulting Ltd Richard Young Managing Director		17 July 2018