BIOMETRICS INSTITUTE LIMITED

DATA PROTECTION POLICY

The Biometrics Institute is committed to upholding your privacy as a valued member, prospective member, stakeholder or user of the Biometrics Institute services. The following document sets out the general rules and protocols which apply to data protection at the Biometrics Institute. The Biometrics Institute is a member-based association operating globally in a multijurisdictional environment with regards to privacy and data protection. Its business operations include collecting, storing, processing and transacting data relating to its members and prospective members. The document includes measures the Biometrics Institute will take as soon as practicable as well as compliance and notification steps as soon as it is aware that there are reasonable grounds to believe there is an eligible data breach.

In dealing with external parties, the Biometrics Institute adopts the following principles:

1. The Biometrics Institute is governed by local privacy regulation e.g. EU's General Data Protection Regulation (GDPR), British Privacy law which mirrors the GDPR and the Australian Privacy Act.
2. We will collect only the minimum amount of personal data required to provide a service to your organisation
3. We will do our utmost to collect, process, store and transfer personal data in an effective and responsible manner. This will include IT equipment being secured, audits being conducted, appropriate logs kept, checks on the system security being conducted from time to time and privacy impact assessments being conducted when significant privacy impacting new business is being planned.
4. We will not sell any personal details to third parties for promotional or other commercial purposes.
5. Personal details will not be sent to, nor processed in, countries where a less stringent privacy jurisdiction is applied.
6. In keeping with the key privacy protection principle "the right to be forgotten", the Biometrics Institute will maintain personal data only as long as necessary. Should we receive a request that the organisation's active participant/s should be deleted from our record, we will do so.
7. Individuals in their own right or as individuals who have authority to sign for their organisation should give informed consent when they provide their personal data; that includes the right to know how their own data will be used by the Institute.
8. We have in place a Board-approved Data Breach Notification process so that in the urgent situation that follows a data breach, everyone knows what to do.
9. We have a Data Protection Officer who is responsible for dealing with your queries and ensuring good privacy practice. This is Laura Compton, Chief Operating Officer.

CONTENTS

CLAUSE

SCHEDULE

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we may collect, store and process personal data about our members, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data is required to maintain confidence in our organisation and our business practices.

1.2 All data users associated with the Biometrics Institute are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action or legal recourse.

2. ABOUT THIS POLICY

2.1 The types of personal data that the Biometrics Institute (We) may be required to handle includes information about current, past and prospective members, suppliers, collaborators and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in various legislation in countries in which we operate in, including the General Data Protection Regulations (EU).

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 The Data Protection Officer is responsible for ensuring compliance with the privacy regulations in which our data is processed or stored and with this policy. \Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

2.6 The *Schedule of Roles* identifies specific individuals responsible for various elements of this policy.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK, Australian or other national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with this policy. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on Biometrics Institute's behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, sexual life or sexual preference, about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings, and genetic or biometric data for the purpose of uniquely identifying a natural person.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Secure.

(h) Not transferred to people or organisations situated in countries without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 This Policy is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in this Policy. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met as outlined in Section 6 and elsewhere in this Policy statement. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. PROCESSING FOR LIMITED PURPOSES

6.1 In the course of our business, we may collect and process the personal data set out in the **Error! Reference source not found.**. This may include data we receive directly f rom a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

6.2 We will only process personal data for the specific purposes set out in the *Schedule of Data Processing Activities* or for any other purposes specifically permitted by this Policy. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. NOTIFYING DATA SUBJECTS

7.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. ACCURATE DATA

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards such as during membership renewals. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. TIMELY PROCESSING

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller (see also clause 15).

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended (see also clause 9).

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

12. DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if the processor agrees to comply with the

Biometrics Institute procedures and policies, or those that are verified to be comparatively equivalent.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on Biometrics Institute's central computer system instead of individual PCs.

12.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the Office Manager or local security team.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock or log off from their PC when it is left unattended.

13. TRANSFERRING PERSONAL DATA TO ANOTHER COUNTRY

13.1 We may transfer any personal data we hold to a country outside the country in which it was collected, provided that *one* of the following conditions applies:

(a) The country to which the personal data are transferred ensures a level of protection for the data subjects' rights and freedoms consistent with the country in which it was collected.

(b) The data subject has given his consent.

(c) The transfer is necessary for the performance of a contract between the Biometrics Institute and the data subject, to facilitate a service requested by the data subject (such as event registration), or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data

subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

13.2 Subject to the requirements in clause 12.1 above, personal data we hold may also be processed by staff operating outside the country in which it was collected, who work for us or for one of our suppliers. Those staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

14. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

14.1 We may share personal data we hold with any member of our Group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

14.2 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

(c) If necessary for the delivery of goods or services as requested by the data subject (such as registering for an event).

14.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.4 We may also share personal data we hold with selected third parties for the purposes set out in the *Schedule of Data Processing Activities*.

15. DEALING WITH SUBJECT ACCESS REQUESTS

15.1 Data subjects may make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Data Protection Compliance Manager immediately.

15.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be verified during the telephone call.

15.3 Our employees will refer a request to the Data Protection Compliance Manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

16. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Schedule with Examples of Data Processing Activities

Type of data	Type of data subject	Type of processing	Purpose of processing	Type of recipient to whom personal data is transferred	Type of recipient to whom personal data is transferred
Contact details	Member, Supplier, Collaborator, third party, advisor	Storing	Update about Member Services, conferences, news and information		Period of membership (if member) and three years
Contact details, DOB, NI number, marital status, sickness record	Employees, consultants, interns, volunteers, officers	Storing	Discharging duties as employer	Advisors	Length of engagement plus 3 years

Schedule of Roles

Role	Name	Phone #	Email	Address	Date Last Verified
Data Protection Officer	Laura Compton (COO)	+44 7926 343955	laura@biometricsinstitute.org	8 Kean St, Imperial House, London WC2B 4AS, UK	6/3/19
Office Manager	Christine Rogers	+61 2 9431 8688	christine@biometricsinstitute.org	Level 3, 33-35 Atchison Street, St Leonards NSW 2065, Australia	15/4/18
Chief Executive	Isabelle Moeller	+44 7887 414 887	isabelle@biometricsinstitute.org	8 Kean St, Imperial House, London WC2B 4AS, UK	15/4/18