Staff Data Protection Policy

1. Background

1.1 GCC Board Directors Institute ("**GCC BDI**", "**we**", "**our**" or "**us**") keeps certain information about its employees, members, suppliers, event attendees, job candidates, clients, founders, strategic partner, corporate affiliates, sponsors and others to allow it to manage its membership, services, business and monitor its performance. It is also necessary to process information so that GCC BDI can comply with its legal obligations and for a variety of business purposes. In order to comply with the applicable data protection laws, including General Data Protection Regulation 2016/679 ("**GDPR**") and DIFC Data Protection Law No. 5 of 2020 ("**DIFC Data Protection Law**") personal data must be collected and used fairly, stored safely and not disclosed unlawfully. This Data Protection Policy ("**Policy**") contains information on how to collect, use, store and dispose of personal data on our systems.

1.2 The DIFC Data Protection Law and the GDPR place an obligation upon GCC BDI, as a data controller, to collect and use personal data in a responsible and accountable manner. GCC BDI is committed to ensuring it complies with the applicable data protection laws regarding all individuals whose data is processed by GCC BDI.

1.3 Words used in this Policy have the same meaning as set out in the applicable data protection laws.

2. Basic principles

2.1 The basic principles which apply to the processing of personal data are that personal data shall:

(a) be obtained and processed fairly, lawfully and in a transparent manner;

(b) be obtained for specified, explicit and lawful purposes and shall not be processed in any manner incompatible with that purpose;

(c) be adequate, relevant and limited to what is necessary in relation to the purpose;

(d) be accurate and kept up to date;

(e) not be kept for longer than is necessary for that purpose;

(f) be processed in accordance with the data subject rights; and

(g) be kept secure from unauthorised access, accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Data controller

3.1 GCC BDI is a data controller as specified in the applicable data protection laws, and the Board of GCC BDI is ultimately responsible for implementation. However, the Data Protection Manager will deal with day-to-day data protection compliance matters.

4. Compliance

4.1 GCC BDI and all its employees, contractors, temporary workers and consultants (collectively referred to as "**staff**" or "**you**") or others who process or use personal data must ensure that

they follow the applicable data protection laws at all times. In order to ensure that this happens, GCC BDI has developed this Policy.

4.2 Any staff, who considers that this Policy has not been followed or has any questions about this Policy, should contact the Data Protection Manager. The Data Protection Manager has overall responsibility for this Policy.

4.3 If and when, as part of their responsibilities, staff collect information about other people (e.g. members, other staff), they must comply with this Policy.

5. Status of this Policy

5.1 This Policy does not form part of the formal contract of employment for staff, but it is a condition of employment that all staff will abide by the rules and policies made by GCC BDI from time to time. Any failures to follow the Policy can therefore result in disciplinary proceedings.

5.2 We may supplement or amend this Policy by additional policies and guidelines from time to time, and we will inform you of material changes. It is your responsibility to check the GCC BDI website policy page regularly or the most recent version of this Policy.

6. Your Personal Data

6.1 All staff are responsible for:

(a) checking that any information that they provide to GCC BDI in connection with their employment is accurate and up-to-date; and

(b) informing the Accounts and Administration Manager of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently.

7. Lawful, fair and transparent processing

7.1 We must process personal data lawfully, fairly and transparently in accordance with individuals' rights. Generally, this means that we should not process personal data unless:

(a) the processing is necessary to perform a contract or provide a requester service (including an employment contract);

(b) the processing is necessary to perform our legal obligations;

(c) the individual has clearly consented to their information being processed; or

(d) we have a clear legitimate business interest, taking into account the rights of the individuals.

7.2 There may be other limited circumstances in which GCC BDI may have an alternative legal basis for processing personal data.

7.3 When relying on consent, it must be freely given, specific, informed and unambiguous, and given by a statement or by a clear affirmative action which shows that the individual agrees to the processing of their personal data. Records of consents should be maintained and if someone withdraws their consent to processing their information, you must stop processing it and notify the Data Protection Manager. Additionally, measures must be implemented to

assess the ongoing validity of consent to ensure that where an individual would no longer reasonably expect the processing to be continuing, the individual should be contacted without delay and asked to re-affirm such consent.

7.4 Under the applicable data protection laws, we are required to provide certain information to individuals relating to the processing of their personal data. Our Privacy Policy, Website Terms and Conditions and Privacy Notice for Employees contain such information and should be directed or provided to individuals at the time of collecting their personal data. The information required by applicable data protection laws to be provided includes:

(a) a statement that the GCC BDI is the data controller;

(b) the name and contact of the Data Protection Manager;

(c) a clear explanation of the types of data being collected and the purposes for which that data will be processed;

(d) the legal bases for processing and how long personal data will be retained for;

(e) any further information that is considered necessary to ensure that the data processing is transparent, for example:

(i) details of any third parties to whom the data might be disclosed;

(ii) details of any transfers of personal data out of the DIFC (including mainland UAE);

(iii) where the processing is based on consent, the right to withdraw such consent at any time;

(f) the right to lodge a complaint with the applicable data protection regulator;

(g) whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply;

(h) the existence of the right of access to and other rights that individuals have to the personal data that we hold about them; and

(i) whether the personal data will be used for direct marketing purposes. Data subjects must be provided with the above information.

8. Special Category Personal Data

8.1 Special category personal data are considered to be sensitive under the applicable data protection laws and include personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.

8.2 In some cases, GCC BDI may process special category personal data related to your employment and/or where we are required to do this by law and/or it is necessary for the purpose of carrying out GCC BDI's legal obligation as an employer and exercising the specific rights of GCC BDI as a data controller.

9. Data Security

9.1 Of fundamental importance within any data protection regime is the security of the personal data that is being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside of GCC BDI without their permission. GCC BDI must keep personal data secure against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

9.2 GCC BDI has an obligation to implement appropriate technical and organisational measures to ensure that data remains secure. All staff are responsible for ensuring that in relation to personal data:

(a) they comply with GCC BDI's IT Security Policy;

(b) any personal data that they hold is kept securely (e.g. by complying with rules on access to premises, computer access, password protection, file storage and other related measures);

(c) they only access personal data that they have authority to access and only for authorised purposes;

(d) personal data is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party;

(e) they do not remove personal data or devices containing personal data (or which can be used to access it) from GCC BDI's premises unless appropriate security measures are in place such as encryption, pseudonymisation, anonymisation or password protection to secure the information and the device; and

(f) they do not store personal data on personal devices or local drives.

9.3 Each staff whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage, in line with this Policy and the IT Security Policy.

9.4 Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

10. Safekeeping of information

10.1 Personal data should:

(a) Be kept in a locked filing cabinet, drawer, or safe; *or*

(b) If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and

(c) If a copy is kept on any type of removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

11. Secure processing of personal data

11.1 While staff in the course of performing their legitimate duties are using personal data, reasonable precautions must be taken to ensure the safety and privacy of that data. For example:

(a) in open-plan offices, computer screens that could potentially be displaying personal data should not be positioned such that unauthorised persons may readily see that data, and all PCs should be password protected;

(b) personal data in manual form, such as in paper files, correspondence or database printouts, should not be left in view in open-plan offices while the relevant staff members are away from their desks. They should instead be locked away or at least covered;

(c) where manual records containing personal data are accessible to a number of staff they must not be removed from the office and should always be returned at the end of the day to their proper place; and

(d) where company laptops are used for working from home, or off-site, the same precautions should be taken by employees as if they were working in the privacy of the GCC BDI office.

12. Authorised and unauthorised disclosures

12.1 Staff working with personal data must be made aware of the purposes for which the data is processed and the legitimate parties either within or outside GCC BDI to whom that data, either in whole or in part, may be disclosed or transferred.

12.2 Personal data must not be disclosed either orally or in writing or via Web pages or by any other means, manual or electronic, accidentally or otherwise, to any unauthorised third party.

12.3 Personal data should never be stored off site in manual form, unless as part of the company's business continuity procedures or with written permission.

12.4 Staff should be aware that log files would record details of all users who access, alter or delete or attempt to access, alter or delete centrally held computerised databases and files containing personal data.

12.5 Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

13. Security of data during transfer

13.1 Where personal data is transferred within GCC BDI and/or to any external third parties in the course of their legitimate activities, staff should be aware of the sensitive nature of such personal data and ensure the appropriate level of security such as password protection and encryption.

14. Disclosures outside GCC BDI

14.1 In general, no personal data should be amended or disclosed to an individual and/or organisation outside GCC BDI unless the authority of the individual who has requested the

amendment or disclosure can be verified. Where a request to disclose or amend personal data relating to a staff member or member of GCC BDI is requested (e.g. by those claiming to be PAs, relatives or friends of the concerned individual), it should be refused unless the consent of the data subject is obtained for such disclosures or in one of the few situations where disclosure without consent is permitted by the law.

14.2 Requests for the disclosure of personal data from the Police, Government bodies, or other official bodies and agencies should be investigated sufficiently to verify the authenticity of the request and may then be acted upon if there is a legal requirement for such disclosure or the consent of the data subject has been given for the disclosure.

14.3 In all cases mentioned in section 14, the permission of the Data Protection Manager is required.

15. International Transfers

15.1 Transfers of personal data outside of the DIFC (whether to a UAE onshore entity or to another country) are not permitted unless:

(a) it is necessary to perform a contract with the data subject;

(b) the data subject has given their explicit prior written consent after being informed of the risks of such transfer;

(c) appropriate safeguards are in place such as standard contractual clauses (please contact the Data Protection Manager for details); or

(d) the country is on the DIFC Data Protection Commissioner's approved list (please contact the Data Protection Manager for details of approved countries).

15.2 Staff should be careful when looking to use suppliers who are based outside the DIFC and seek advice from the Data Protection Manager.

16. Amendment and Accuracy of personal data

16.1 Staff should ensure that the personal data that we process are accurate, adequate, relevant and not excessive given the purpose for which the data were obtained.

16.2 From time to time data subjects will wish to update some of their personal data held by GCC BDI, for example their home addresses or other contact details previously submitted. To do this, the data subjects must provide GCC BDI with their updated data and the GCC BDI staff handling this data must satisfy themselves that of the proof of identity of the data subject.

16.3 With the introduction of GCC BDI 'self-service' web-based administrative systems for staff and members, the data subjects themselves are able to take responsibility for the maintenance of certain elements of their personal records. These systems incorporate the necessary authentication and security mechanisms to ensure that data subjects are only able to view and amend their own data.

16.4 Regular checks should be undertaken to ensure that personal data are accurate and up-to-date and that the minimal data required is collected.

17. Publication of GCC BDI Information

17.1 The names and some biographical information of Board Directors, staff, faculty and members of GCC BDI may be published in the Annual Report and on GCC BDI's public website and newsletter and in any other documents where any statute or law requires SUCH DATA TO BE MADE PUBLIC.

18. Retention of Personal Data

18.1 GCC BDI must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances, taking into account the purposes for processing the personal data. Please refer to the Data Retention Policy for detailed information. GCC BDI has a duty to retain some employee and member personal data for a period of time following their departure or resignation from the company, mainly for legal reasons, but also for other purposes such as financial reasons e.g. external audits. Such data will be retained for as long as either the law requires or a maximum of 10 years whichever is shorter, unless the data is required for the GCC BDI archives.

18.2 While the majority of personal data held by GCC BDI is processed for internal administrative purposes and is never disclosed outside the institute, some categories of data are routinely or from time to time released through one or more forms of publication such as:

(a) GCC BDI Website

(b) GCC BDI Newsletter

(c) Annual Report

(d) Directors' Register

(e) Disaster Recovery and Business Continuity Plan

18.3 Data subjects are informed of GCC BDI's obligations and policies in this respect at the time the data is collected (see Privacy Policy).

19. Disposal of personal data

19.1 When a record containing personal data is to be disposed of, the following procedures will be followed to ensure that personal data are disposed of securely:

(a) all paper or microfilm documentation containing personal data will be permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data; and

(b) all computer equipment or media that are to be sold or scrapped will have had all personal data completely destroyed, by re-formatting, over-writing or degaussing.

19.2 Staff will be provided with guidance as to the correct mechanisms for disposal of different types of personal data. In particular, staff will be made aware that erasing/deleting electronic files does not equate to destroying them. If it is possible to de-identify the information such that specific individuals cannot be identified from it, we may be able to keep this for longer, for example, where this is useful for analytical or statistical purposes.

20. Data Breaches

20.1 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 transmitted, stored or otherwise processed. Under the applicable data protection laws, GCC BDI is required in certain circumstances to notify regulators (potentially within 72 hours and without undue delay) and/or affected individuals about data breaches.

20.2 Therefore all staff have an obligation to report actual or potential data protection compliance failures as soon as they become aware of them. This allows GCC BDI to investigate, mitigate and notify any authorities or individuals as necessary. It is very important that staff do not delay in reporting a data breach as time is critical in this regard. If you become aware of a data breach or a suspected data breach, you must notify the Data Protection Manager immediately.

21. Data Subject Requests

21.1 Under the applicable data protection laws, individuals including staff and members have certain rights in relation to their personal data. This includes requesting access to a copy of personal data being kept about them at GCC BDI either on computer or in certain files (subject to certain exemptions).

21.2 Individuals also have rights in certain circumstances to request rectification, erasure, restriction, data portability, to object to processing, to non-discrimination and other rights in relation to automated decision-making and profiling.

21.3 If you receive a data subject request, refer that request to the Data Protection Manager immediately as the law generally requires us to respond to data subject requests within one month of receiving the request.

21.4 GCC BDI, will, upon receiving a data subject access request, verify the identity of the data subject and provide the data subject with a copy of personal data processed by GCC BDI in electronic form, as well as a statement regarding the personal data held about them. This will state all the types of personal data which GCC BDI holds and processes about them, the purposes for which they are processed and the recipients or categories of recipients to whom personal data are disclosed. The information will need to be reviewed by the Data Protection Manager to consider whether any relevant exceptions apply and to ensure no third party personal data are disclosed.

21.5 Any person who wishes to exercise this right should complete the Subject Access Request Form in Appendix 1 and this and submit it to the Data Protection Manager at getinvolved@gcbdi.org. GCC BDI aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month.

21.6 No data subject rights are absolute; there are certain exceptions and restrictions on the information to which a person is entitled or what they can require an organisation to do in response to a request under applicable data protection laws.

22. Processing of personal data within GCC BDI Activities – Specific Purposes

22.1 GCC BDI cannot simply collect personal data for reasons to be later determined. Staff should ensure personal data are only collected for specific purposes and should not later decide to use that personal data for other reasons. Listed below are the activities carried out by GCC BDI

that involve the processing of personal data. This list is non exhaustive and it is the responsibility of the Data Protection Manager to ensure that all staff receive sufficiently detailed guidance to enable them to carry out these activities in accordance with the requirements of the applicable data protection laws and this Policy:

(a) Membership applications and management

(b) Directors Register

(c) General enquiries

(d) Events/conference administration

(e) Publications eg Website, Newsletter, Annual Report

(f) Marketing including fundraising activities/donor administration etc

(g) Research activities and administration

(h) Staff management (includes performance, appraisal and development records, leave

(i) Records, expenses records, etc

(j) Staff recruitment

(k) Systems administration (e-mail, back-up/ storage, authentication, system logs, etc)

(l) Trainers, facilitators and presenters activities and administration

(m) Finance administration (includes payroll, banking, VAT, taxes, benefits, auditing)

(n) Health and Safety

(o) CRM and Mailing list administration and use

(p) Legal administration eg DIFC portal, residence visas

(q) Market research

(r) News/press release activities/public relations and other publication activities

23. Specific rules - marketing

23.1 There are specific rules relating to marketing to individuals electronically (e.g. by email or SMS). These rules may vary depending on where the individual is located (e.g. in Europe, DIFC or mainland UAE). GCC BDI is generally not permitted to send direct marketing material to individuals unless they have consented to receiving those communications from us, although there may be some exceptions to this.

23.2 You should promptly comply with any request from an individual not to use their personal data for direct marketing purposes and notify the Data Protection Manager about any such request.

23.3 Contact the Data Protection Manager for advice on direct marketing before starting any new direct marketing activity.

24. New technologies, services and processes

24.1 When designing and planning on implementing new technologies, services, processes and systems or making any changes that could have an impact on individuals' personal data, staff should contact the Data Protection Manager and ensure that:

(a) data protection impact assessments ("**DPIAs**") are undertaken where any high risk processing is to be undertaken. For example, processing which involves special category personal data, profiling or automated decision-making, or scoring; and

(b) a 'data protection by design and by default' approach is taken from the outset to ensure that data protection principles are complied with, and that any data protection concerns are considered and addressed at the design stage and by default.

25. Records

25.1 GCC BDI is required to keep certain written records of its data processing activities. The Data Protection Manager will be responsible for keeping the record of data processing activities and may need to work with the relevant departments to maintain such records.

26. Training

26.1 All staff will receive training on this Policy and the applicable data protection laws, including any new joiners to GCC BDI. Completion of this training is compulsory.

26.2 The Data Protection Manager will monitor training and maintain records of training. If you have any questions, please contact the Data Protection Manager.

27. Conclusion

27.1 Compliance with the applicable data protection laws is the responsibility of all GCC BDI staff. Any deliberate breach of this Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

27.2 Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Manager at getinvolved@gcbdi.org and/or by telephone: +971 (4) 554 7967.

Appendix 1

Data Subject Access Request Form

1. Details of the person requesting the information.	
Full name:	
Address:	
Telephone number:	
Fax Number:	
Email:	
2. Are you the Data Subject?	YES/NO
(a) **IF YES PLEASE COMPLETE THIS SECTION. ELSE PROCEED TO SECTION (b)**	
If you are the Data Subject please supply evidence of your identity i.e. ID card or Passport.	
Please tick appropriate box	
I am a current/former member of staff	
I am a current/former member	
I am neither of the above	
Please now go to question 5.	
(b) **IF NO**	
Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed.	

Please also state the relationship of the Data Subject to GCC BDI:	
The Data Subject is a current/former member of staff	
The Data Subject is a current/former member	
The Data Subject is neither of the above	
Please now go to questions 3 and 4.	
3. Details of the Data Subject (if different from 1.)	
Full name:	
Address:	
Telephone number:	
Fax Number:	
Email:	
4. Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.	
5. If you wish to see only certain specific document(s), please describe them.	
6. If you would like a more general search, please note that GCC BDI is able to search the following sections for personal data. Please	

indicate the sections that you would like searched:	
• Members Register	
• Directors Register	
• Human Resources	
• Finance	
• Administrative files and information	
• Other	
7. Declaration	

I, ……., certify that the information given on this application form is true. I understand that it is necessary for GCC BDI to confirm my/the Data Subject's Identity and it may be necessary for more detailed information to be obtained in order to locate the correct information.

Signed:……

Date:……

Please return the completed form to the Executive Directors, GCC Board Directors Institute, 2201 South Tower, Emirates Financial Towers, DIFC, Dubai, UAE

or send by email to getinvolved@gcbdi.org

Document updated 18 December 2021