BCS, The Chartered Institute for IT

Member Group Data Protection Policy and Procedures

April 2018

CONTENTS

1.   Background

This policy is designed to minimise risks while maximising our functionality.

GDPR, Regulation (EU) 2016/679, imposes significant sanctions on organisations who breach data protection law.

Volunteers are extremely important to the functioning of BCS and this policy reduces the amount of risk that our volunteers take on during the day-to-day running of their groups.

A data protection breach can carry fines of up to £16m (EUR20m); fines far larger than have existed before.

Under data protection law, both the outgoing Data Protection Act 1998 and the incoming GDPR, BCS has an obligation to all of the data subjects whose data is processed by us to ensure that operational measures are taken to ensure the security, safety and privacy of the personal information we use to provide services to our members and ensuring the rights and freedoms of all data subjects who entrust their data to BCS.

The damage that can be caused to individuals, the reputation of BCS and to volunteers is significant and BCS has a responsibility to ensure that we take every reasonable step to prevent things going wrong.

Any members who operate outside of these instructions shall face disciplinary procedures under the BCS Code of Conduct.

2.   Definitions

"Data Protection Law" means the Data Protection Act 1998, Privacy and Electronic Communications Regulations (PECR), General Data Protection Regulations (EU) 2016/679 and the Data Protection Bill 2017.

"Data Processing" is any action carried out on personal data.

"Personal Data" is any information that can be used to identify a natural living individual.

"Data Subject" is any individual who is the subject of personal data

"Data Controller" is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.   Purpose

This policy has been created to ensure that BCS, The Chartered Institute for IT is compliant with its obligations under Data Protection law.

BCS is the data controller for member and non-member data processed within the BCS Group and it has a responsibility to its members and non-members to maintain the safety and security of their personal data.

Groups who operate outside of this policy will be subject to the disciplinary processes set out in the Member Group Rules on the Volunteer Portal.

4. Access to Data

Members and non-members' personally identifiable data is not made available or accessible directly to volunteers within the Member Groups. Committee volunteers within Member Groups may request Business Intelligence reports covering a wide range of useful information such as member joining/leaving numbers, age ranges and location data. This information is currently available on a request basis to your Community Coordinator at Swindon office.

This information shall contain no personal data but will provide you with key statistical information needed for matters such as preparing for and running annual general meetings and the planning and co-ordination of events.

Requests for reports are typically processed within five working days.

5. Member Group Communications

It is key that Member Groups can contact their constituent members and inform members about events and news relating to the group.

All electronic message broadcasting will be carried out via the list servers provided. Nominated committee members, who hold professional membership of BCS, are given access to post to these lists directly without the need for interfacing with the BCS Community team.

The data in our membership database, including non-member lists will be processed and managed by the BCS Community team. Unsubscribe preferences can be managed directly by the individual member via the member secure area (MyBCS), or by request via BCS Customer Service or the BCS Community team.

Individual committee members may hold contact details of their fellow committee members in much the same way you have the contact details for colleagues at your place of employment. Where they have consented to provide you their contact information for these purposes, BCS holds no legal responsibility over this data.

All other activities such as marketing for events, newsletters, callouts for AGMs, additional benefits, or general group updates must be done via the list servers or via your Community Coordinator.

6. Events

BCS Member Groups must use the central BCS Eventbrite account for running their events.

Eventbrite is an external service operated on servers in the United States, processed under the EU-US Privacy Shield. Users register with Eventbrite to make bookings and this information is returned to BCS.

Each Member Group is required to complete an event booking request form in order for a BCS Community Coordinator to set up the event listing on Eventbrite in an approved format.

All events for which attendees must pre-register to attend must be created and managed by your Community Coordinator.

Contact your Community Coordinator to set up the event on the BCS approved booking systems and manage pre- and post-event communications.

For events that are open attendance with on-the-day sign-in, you must use the sign-in sheet provided on the Volunteer Portal.

This sheet must be returned, password protected or encrypted, to the Coordinator within three days of the event. The password for files must be sent in a separate communication, ideally by an alternative communication – e.g. by phone call or SMS text message – to the file itself. The hardcopy of the sheet must be destroyed after confirmation of receipt from the Coordinator. The Coordinator will log the contact details of non-members who have agreed to receive future communications in the list server.

7. Non-Member Registration

Non-members are permitted to join mailing lists and attend BCS Member Group events. Collection of their data shall be done centrally via the Member Group's webpage on the BCS website.

Non-members can request to be removed at any time, either by following the instructions in any of the emails sent or by contacting the Customer Service team.

8. Data Subject Rights

Any enquiries about personal data from your member group participants should be directed to the Swindon office, either via the Community Coordinator or via the Customer Service team.

9. Notification of a Breach

You must notify the Legal Services team immediately upon discovery of a possible data protection breach. BCS has 72 hours to notify the Information Commissioner's Office (ICO) in the event of a breach so there can be no reason for delay.

You can notify the legal team at **legal@bcs.uk**

10. Got a question?

Not sure about something or think there's something we've missed?

Please first check the Frequently Asked Questions document but if there is something that isn't covered there, contact your Community Coordinator who will pass the enquiry on further.

11. Policy Review

This policy shall be reviewed annually in consultation with the Community Board.