

GDPR

Member Data Policy

15th March 2018

Who am I?

Martyn Cox
BCS, The Chartered Institute for IT



Legal Administrator & GDPR Project Lead

Bachelor in Laws from Swansea University

Joined BCS in November 2015

70 days to go

The General Data Protection Regulations will come into force on 25 May 2018

What are we trying to achieve?



- Discharging our legal and moral responsibilities to our members and others ...while spending no more than we have to
- Help volunteers and staff play their roles ...while minimising the personal risks to our volunteers
- Avoiding a 'killer' risk to BCS ...while ensuring we can do as much of what we need to as easily as we need to

A difficult balancing act many organisations are going through

The story so far...

- November 2016: Presented at the Role Based Convention on GDPR and the implications for BCS, received initial feedback
- January 2017: Data Handling Survey taken of all member groups. 77 respondents
- February 2017: Internal Compliance Project set up
- Summer 2017: Internal Compliance focus
- September 2017: Data Protection Impact Assessment taken based on information provided in survey and on processes demonstrated by Community Co-Ordinator team
- October 2017: First draft of policy
- November-December 2017: Internal reviews and adjustments made.
- January 2018: Policy sent to Community Board and Best Practice Committee for review, feedback taken
- February 2018: Consultations held with Iain Thompson and Alastair Revell
- March 2018: Eighth draft and full member group consultation

Policy backdrop: evolving picture for GDPR regulations / implementation

Policy Rationale



- GDPR, Regulation (EU) 2016/679, imposes significant sanctions on organisations and individuals who breach data protection law.
- This policy is designed to meet our compliance obligations, minimise the risks to volunteers when processing personal data and ensure that our groups are still able to function.
- 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 of such significance that even one significant breach would mean that BCS would have to fold.
- 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.

The Policy Objectives

Risk Identification

Risk Register: Member Groups Data Protection Impact Assessment

- Personal Data shared externally to non-BCS employees and non-contracted volunteers (Third parties)
- No direct control over how personal data is processed by member groups
- Inconsistency in processing across groups and lack of transparency over what is happening with personal data
- Cannot ensure information security
- Non-standard data collection across different groups
- Inconsistent event and attendee data management

Associated Corporate Risk

- Reputational
- Regulatory
- Financial
- Legal

The Policy Objectives

Aims

Security

Transparency

Consistency

Accountability

Identifying Solutions

- BCS central functions to manage and handle the majority of data processing with guidance given on limited processing carried out by group functions
- Better evidence and management of consent, consent revocations and deletion of data
- Evidencing to ICO what processing occurs within the organisation
- Limit the dissemination of bulk personal data to contracted BCS employees, and minimise within the staff team as well
- Standardise processes across all member groups so that we can be clear to the ICO, and manage deletions etc.
- Provide central systems for event booking – Eventbrite - and provide a process for managing attendance reporting
- Standardise data collection so that privacy notices will be correct and truthful
- Provide transparency about the processing of a member's data
- Ensure all marketing communications are done centrally and have the required privacy statements in them

Policy Consultation



- We clearly have no option but to change, and aspects of the law dictate the limited range of solutions available to us to continue member group functions
- We have our solutions ready to go, we've consulted, evaluated impact on groups, plans in place...
 - ...but...we want to hear if we've missed anything!
- As part of the post-convention survey, there will be questions about the policy and a call for comment/suggestions...which we have to act on quickly.
- We want you to bring forward ideas of how we can do things differently with this policy while still maintaining security, transparency, consistency and accountability
- We will provide feedback on ideas and potential solutions and work collaboratively to bring a resolution.
- The policy needs to be implemented following by April 16th in order for processes to be changed and implemented by May 25th.
- This policy will be under regular review over the next two years, but we will always be listening!

Final thoughts



- GDPR is coming and the changes we are having to make are a necessity. Every organisation is having to adjust, and take difficult calls on compliance.
- Work with us and we can find a resolution and make sure that BCS and its volunteers are able to continue Making IT Good for Society in the GDPR world
- This isn't just BCS, this affects every business, organisation and individual who works with personal data.