Data Protection
Policies and Procedures

Table of Contents

APPENDICES

1.0 Introduction.

1.1 The Data Protection Act 1998, as updated by the General Data Protection Regulation 2018, establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. The Act, together with principles and procedures, imposes obligations on BTG and its Data Controller, with regard to the purposes for which Personal Data is processed, the classes of Data, the Data Subject, recipient and the transfer of Personal Data outside of the European Economic Area (EEA).

1.2 BTG collects and holds personal data on the basis of legitimate interest.

1.3 The Named Representative for data protection purposes within BTG is the Chair of the Committee who is responsible for notifying the Information Commissioner that BTG processes Personal Data.

BTG's notification covers the following purposes:

- Advertising, marketing and public relations
- Accounting and auditing
- Service User administration
- Member administration.

2.0. Purpose

To ensure that the standards required by BTG and the statutory regulations are adhered to and the required levels of compliance are achieved and maintained.

3.0. Scope

This policy and associated procedures apply to all members, contractors and consultants who work for BTG under a contract for services, supporters of the organisation and service users of BTG.

4.0. Definitions

DATA is information which:

i. is being processed by equipment operating automatically in response to instructions given for that purpose;

ii. is recorded with the intention that it should be processed by means of such equipment; or

iii. is manually input into records held on computer systems or paper records

iv. is recorded as part of a Relevant Filing System or with the intention that it should be part of a Relevant Filing System.

In the case of information that does not fall under above categories, data will also include information which forms part of an accessible record such as a health, educational or accessible public record.

PERSONAL DATA is Data relating to a living individual who can be identified from the Data or other information in the possession of (or likely to come into the possession of) BTG.

SENSITIVE PERSONAL DATA is Data which requires the explicit (i.e. written) consent of the Data Subject before processing can take place, and is Personal Data consisting of information as to the Data Subject's: -

• racial or ethnic origin

• political opinions, religious or other beliefs

• trade union membership

• physical or mental health or condition

• sexual life

• commission or alleged commission of any offence

• proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentencing of any court in such proceedings.

MANUAL DATA is Data which forms part of a Relevant, Non Electronic, Filing System.

RELEVANT FILING SYSTEM is any set of information which is not processed by means of equipment operating automatically relating to individuals and structured, either by reference to their name or to a criterion relating to them (i.e. name of employee or service user, National Insurance number, payroll number etc) in such a way that specific information relating to them is readily accessible.

PROCESSING means obtaining, recording, holding or carrying out any operation on the information including organising, adapting, altering, retrieving, consulting, disclosing by transmission, using, amending, disseminating, aligning, combining, blocking, erasing or destroying.

FAIR PROCESSING means BTG must be open about why it wants the information as well as having a legitimate reason for processing it by stating in writing the name of the Data Controller, what it intends to use the information for and to whom it intends to give or share it.

DATA CONTROLLER is an individual or organisation who determines the purposes for which and manner in which any Personal Data is being or will be processed.

NAMED REPRESENTATIVE is an individual nominated by BTG who is responsible for notifying the Information Commissioner regarding the organisation's use of Personal Data. (i.e. the Chair of the Committee).

DATA SUBJECT is an individual who is the subject of the Personal Data.

DATA PROCESSOR is any individual or organisation who processes Personal Data (other than employees of Data Controllers) on behalf of the Data Controller (e.g. pensions, administrators, insurance companies, Payroll providers, etc).

THIRD PARTY is any individual or organisation other than BTG the Data Subject or a Data Processor (excluding employees of the same).

SERVICE USER is any individual who is the recipient of a service provided by BTG.

5.0. Data Protection Principles

BTG has a responsibility as a Data Controller under the Data Protection Act 1998, as updated by the General Data Protection Regulation 2018, to ensure that it complies with the complies with the data protection principles of good information handling practice.

Broadly these state that Personal Data must:

i. Be processed fairly and lawfully

ii. Be obtained only for one or more specified and lawful purposes and not further processed in any way incompatible with those purposes

iii. Be adequate, relevant and not excessive for its purposes

iv. Be accurate and kept up to date where necessary

v. Not be kept longer than is necessary

vi. Be processed in accordance with the rights of Data Subjects

vii. Be surrounded by appropriate technological and organisational measures against unauthorised/unlawful processing, access, accidental loss, destruction or damage

viii. Not be transferred out of the EU without ensuring adequate levels of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data are in place.

6.0 Responsibilities.

6.1 The Committee

6.1.1 To ratify Policy

6.1.2 To receive periodic reports on the organisation's compliance with Data Protection and the level of Data Protection complaints across BTG.

6.2 Named Representative (i.e. the Chair of the Committee)

6.2.1 To review effectiveness of Data Protection policy

6.2.2 To develop business and service continuity plans

6.2.3 To provide leadership and promote responsible attitudes towards Data Protection to all members

6.2.4 To investigate breaches/potential breaches of the Data Protection policy and report findings to the Chair of the Committee and the Committee Members and to the ICO (Information Commissioner's Office)

6.2.5 To review Changed/New Purposes for Personal Data

6.2.6 To ensure data protection information is provided to all committee members and staff on Data Protection policy

6.2.7 To invoke formal Disciplinary Policy where breaches of the Data Protection policy have occurred

6.2.8 To develop secure archiving and disposal systems

6.2.9 To develop best practice approach towards security of Personal Data

6.2.10 To determine level of member access to Personal Data and conduct reviews of such access

6.2.11 To monitor and review data protection practice and compliance, implement improvement plans where required.

7.0. Policies.

7.1 BTG's Data Protection Policy

BTG's policy in respect of its obligations under the Data Protection Act 1998, as updated by the General Data Protection Regulation 2018 [GDPR 2018] are as follows:

7.1.1 To take all practical steps to ensure that the requirements of both the Data Protection Act 1998 and of the General Data Protection Regulation2018 are achieved and maintained throughout the organisation at all times.

7.1.2 To respond to written subject access requests as quickly as possible and no longer than one month from the initial request.

7.1.3 To reserve the right to randomly check e-mails, website use and telephone use, in order to protect itself against unlawful use or access. Such monitoring will be conducted in a lawful and fair manner.

NB Such monitoring is covered by the Data Protection Act 1998, as updated by the General Data Protection Regulation 2018 [GDPR 2018], the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

7.1.4 To investigate alleged breaches of the Data Protection requirements as a disciplinary offence and invoke BTG's Disciplinary Procedure as appropriate.

7.2 Disclosures of Criminal Offences

7.2.1 In addition, changes brought about by legislation, statutory requirements and best practice guidelines (as listed below) place a heavy emphasis on the principles underlying the Data Protection Act, the General Data Protection Regulation and the Human Rights Act with regard to disclosures of criminal offences:

- Police Act 1997
- Protection of Vulnerable Adults Act 1999
- Care Standards Act 2000 (including the Protection of Vulnerable Adults provisions)
- The Care Act 2014
- Disclosure procedure operated by the Disclosure & Barring Service (DBS)
- Relevant Codes of Practice.
- BTG's Statement on Service User Confidentiality and Access to Records.

As such, BTG must emphasise that any improper disclosure of criminal offences would be treated as a very serious disciplinary matter and investigated in accordance with the Disciplinary Policy.

The Care Quality Commission has powers of access and disclosure in accordance with its Code of Practice in Relation to Confidential Information.

8.0. Procedure

8.1 Data Subject Access

8.1.1 All Data Subject requests for access to Personal Data held on them by BTG must comply with the following procedure.

The Data Subject must:

• Complete a 'Request for Access to Personal Data form see Appendix E. However, BTG cannot insist on the data subject using this form. All requests must be in writing including e-mail.

• Provide clear proof of their identity (i.e. NI number, birth certificate, passport, driving licence etc.).

• Specify the type of data to which they require access including which databases/files they require to be searched.

8.1.2 The Data Subject written request must be verified by the Chair. Where appropriate, the Data Subject will be asked if they require copies of the information or merely the opportunity to view it. In circumstances where the Data Subject wishes to view their Personal Data, the Chair shall, so far as is practicable, ensure that the Data Subject is able to do so in private.

8.1.3 Provided the above conditions have been met, BTG will respond to the Data Subject access request as soon as possible and no later than one month of the written request to the Chair.

8.1.4. In certain circumstances Data Subject access request may be refused, for example where:

• Disclosure would include disclosing a Third Party's Personal Data and the Data Controller/Chair does not have their consent to the disclosure of information

• Personal Data requested relates to employment and other confidential references provided by BTG. However, these "received" references may have to be disclosed.

• Personal Data requested is processed solely for the purpose of management forecasting or management planning to the extent that compliance would prejudice the conduct of BTG.

• The Data Subject has not provided sufficient proof of identity, or provided sufficient information with which to locate the Personal Data sought which satisfies BTG.

8.1.5. Where the Data Controller/Chair has confirmed that such access should be refused, BTG will confirm in writing to the Data Subject the reasons for refusing access.

8.1.6 This policy rule ensures that accountability for potential non-compliance in this instance lies with the Data Controller/Chair, not the individual staff member.

8.1.7 Data Subject's wishing to appeal against BTG's refusal to provide access should put their appeal in writing stating their grounds to the Chair as soon as

possible and no later than one month of receiving the letter confirming the decision to refuse access.

Alternatively, concerns can be raised directly with:

The Information Commissioner's Office

Either via:

Helpline: 0303 123 1113 (Mon-Fri, 9am-5pm)

Or

By live chat on their website www.ico.gov.uk

Or

By email: casework@ico.org.uk (please include your telephone number)

8.2 Inaccurate Data

8.3.1 In the event that, following access to their Data, a Data Subject is of the opinion that the information is in any way inaccurate, the Data Subject should notify the Chair of all the errors within the information as soon as practicable.

8.3.2 In addition, where relevant, the Data Subject should notify the Chair of the correct information to replace any inaccurate Data.

8.3.3 Following notification of inaccurate Data, the Chair will, as soon as is reasonably practicable, take the necessary action to correct any inaccuracies.

8.3 Data Transfers

8.4.1 Personal Data must not be transferred to countries outside of the EU.

8.4.2 Further advice on Data transfers may be sought from the Chair.

8.4 Exemptions

8.5.1 The following sets of information are exempt from the Act and, therefore, are excluded from the detailed provisions of this Policy.

Notwithstanding the exemptions listed below, in certain instances the spirit of the Policy will be maintained, so far as is reasonably practicable.

a. Information which BTG is required by law to be made public;

b. Information which BTG is required to be disclosed in connection with legal proceedings

c. Information relating to national security

d. Personal Data processed for the prevention of crime or prosecution of offenders or for the collection of tax.

e. Information relating to any regulatory activity.

9. Photographs or other Visual Material

All members need to be aware that when taking photographs of Service Users appropriate written permission is required from them or their parent/carer. A form exists for this purpose. If any such photographs are subsequently intended for publication (internally or externally) similar written permission needs to be provided. Copies of photographs used should be attached to the form.

Visual Material stored and used for fundraising, marketing and advertising purposes must comply with this policy namely that consent needs to be obtained from the person or their guardian, or organisation supplying the material.

10. Retention of Data

BTG will keep some forms of information longer than others.

- Funding Surveys – 6 years
- Correspondence – 3 years - depending on content (legal elements 6 years)
- Photographs – 2 years (can be extended with express permission)
- Service User records – 6 years from last attendance date (Service users may return after a period of absence, or health/social care organisations may require a record of activities)
- Potential service user records – 6 years from last contact (Individual may become a service user at a future date, so records are useful)

11. Removal of Data

When a Subject (or parent/carer) requests in writing for BTG to immediately delete their data then this should be overseen by the Chair or their designate unless there are legal or special reasons for not doing so. In this case the Chair will first take legal advice.

The removal of data may result in BTG ceasing to provide services to the Subject.

12. Disposal of Data

When personal data is no longer required, or has passed its retention date paper records must be shredded using a cross-hatch paper shredder or by using an approved security shredding company.

Computerised records must be permanently deleted, with particular care that “hidden” data cannot be recovered.

13. Review

13.1 Arrangements to monitor the effectiveness of this policy will be made by the committee.

13.2 This policy will be reviewed every 12 months.

14. Data Security Breach Policy

BTG is committed to taking appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

Data is defined as BTG Personal or Confidential information including intellectual property.

Personal information is defined as any information relating to a living individual who can be identified either from the data, or from that information used in conjunction with other information that may be available.

Confidential information is privileged or proprietary information that could cause harm (including reputational damage) to BTG or individual(s) if compromised through alteration, corruption, loss, misuse, or unauthorised disclosure.

A data security breach is considered to be and can happen for a number of reasons namely:

• Loss or theft of data or equipment on which data is stored

• Inappropriate access controls allowing unauthorised use

• Equipment failure

• Human error

• Unforeseen circumstances such as a fire or flood

• Hacking attack

• 'Blagging' or "Phishing" offences where information is obtained by deceiving the organisation who holds it

However, the breach has occurred, there are four important elements to any breach management plan:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

14.1. Managing a Data Security Breach

Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident.

Apart from the potential punitive financial impact to the organisation, there will be significant reputational risk that will have to be managed by the Board together with the rectification costs in dealing with the technical elements of the breach.

The procedure in Appendices A-D outlines the main steps in managing a breach and will help ensure that all breaches are dealt with effectively and efficiently.

14.2. Record Keeping

Throughout the breach, management process records should be kept of what action has been taken and by whom. An activity log template should be completed to record this information, in addition copies of any correspondence relating to the breach should be retained.

The data breach procedure outlines the four stages which should be completed following the initial containment of the breach. The individual stages may run concurrently.

APPENDIX A

Security Breach Procedures

1. Containment & recovery

As soon as a data security breach has been detected or is suspected the following steps should be taken:

a. Identify who should lead on investigating and managing the breach

b. Establish who (within BTG) should be aware of the breach – the Chair/ Data Controller must be contacted

c. Identify and implement any steps required to contain the breach

d. Identify and implement any steps required to recover any losses and limit the damage of the breach

e. If appropriate inform the Police/Insurance Company

2. Assessment of risk

All data security breaches must be managed according to their risk. Following the immediate containment of the breach, the risks associated with the breach should be assessed in order to identify an appropriate response. The checklist in Appendix B should be used to help identify the exact nature of the breach and the potential severity, this information can then be used to establish the action required.

3. Notification of breach

The Information Commissioner's Office MUST be informed of the Breach asap and latest within 72 hours. They will advise what other action is to be taken. Consideration is required as to whether any individuals, third parties or other persons should be notified of the breach. This will depend on the nature of the breach, any notification must be carefully managed. Do not disclose information before the full extent of the breach is understood; when disclosure is required ensure that it is clear, complete informative. The checklist in Appendix B: Notification of breach checklist should be used to identify such persons who should be notified and to establish what information should be disclosed.

The Chair or Member Advisor must be involved in the notification process and no message should be sent without the Chair of the Committee's approval. The Information Commissioner's Office may be notified only after liaison with the Chair of the Committee or another of the Committee Members.

4. Evaluation and response

It is important to investigate the causes of the breach and evaluate BTG's response to the breach. A brief report on the breach, how it was dealt with and recommendations on how to prevent the breach reoccurring and similar risks should be written. All significant breaches must be reported to the Chair of the Committee.

If there are recommended changes to this procedure, such as additional information that would have been helpful or further explanation required these should be communicated to the DVAs.

Further resources and contact details

For ICO guidance on Data Security Breach Management follow the link:

http://ico.org.uk/for_organisations/data_protection/lose

For ICO guidance and Notification of Data Security Breaches to the ICO follow the link:

http://ico.org.uk/for_organisations/privacy_and_electronic_communications/security_breaches

APPENDIX B

Security Breach risk Assessment Actions

a) What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)

b) How did the breach occur?

c) What type of Data is involved? (The individual data source should be identified and whether the data was sensitive e.g. health records / Bank details etc

d) How many individuals or records are involved?

e) If the breach involved personal data, who are the individuals? (Members, Service Users, Supporters etc)

f) What has happened to the data?

g) Establish a timeline? (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc.)

h) Were there any protections in place? (E.g. Encryption)

i) What are the potential adverse consequences for individuals or to BTG? How serious or substantial are they and how likely are they to occur?

j) What could the data tell a third party about an individual, what harm could this cause? i.e. what is the likely reputational impact?

k) What processes/systems are affected and how? (E.g. web page taken off line, access to database restricted).

A FULL WRITTEN REPORT COVERING THE ABOVE MUST BE PRODUCED AND SHOULD BE DATED AND TIMED.

APPENDIX C

Notification of a Breach - Checklist

Who to notify:

1. The Chair of the Committee
2. Police – in the case of criminal activity
3. Information Commissioner's Office (ICO) - There is a legal obligation to inform the ICO AS SOON AS POSSIBLE but MUST BE WITHIN 72 Hours
4. Individuals whose data has been compromised
5. Other Regulatory bodies, Funders, other third parties e.g. Service User referring agencies - as appropriate
6. Others – e.g. banks where steps may be required to protect accounts.

The Chair of the Committee must be informed as soon as possible.

They will notify the ICO and make the decision in conjunction with the ICO.

The Chair of Committee and the individual responsible for BTG's Press coverage should also be called notified.

Media - WHAT TO SAY

The Chair will be able to advise on the content of any notification. It is important that the extent of the breach is understood, and that useful information is provided, whilst at the same time if there are important steps that individuals need to take this should be communicated promptly.

Consider including the following:

- Details of what happened and when the breach occurred
- What data was involved?
- Has the ICO has been informed?
- What steps have been taken to contain the breach and prevent re-occurrence?
- Advice on what steps they should take e.g. contact banks
- How will you help and keep them informed (if necessary)
- Provide a way to be contacted.

APPENDIX D

Statutory Provisions concerning Data Protection

The statutory provisions – laws – concerning Data protection are: -

• Data Protection Act 1998 (DPA)

• The Human Rights Act 1998

• The Regulation of Investigatory Powers Act 2000 (RIPA)

• The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)

• The Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/ 2905)

• The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)

• The Environmental Information Regulations 2004 (SI 2004/3391)

• The United Kingdom Data Protection (Processing of Sensitive Personal Data) Order 2006 (SI 2006/2068)

The above form the basis for Lindengate's Data Protection Policy & Procedure.

Notes:-

1. The Freedom of Information Act 2000 (FOI Act)

This is only applicable to Local Authorities; it is not applicable to since BTG is an organisation (i.e. not a Local Authority).

2. The Public Interest Disclosure Act 1998

Not relevant to Data Protection as such, however, this Act does protect people against detrimental treatment or dismissal as a result of disclosure of information in the public interest.

APPENDIX E

Request for Personal Data Under the Data Protection Act / GDPR

The Data Protection Act 1998, as updated by the General Data Protection Regulation 2018, provides you ('the Data Subject') with the right to receive a copy of the personal data we hold about you.

This form is used to confirm your identity and to assist us in locating your personal data. This form can also be used to confirm the identity and authority of someone making the request on behalf of the Data Subject.

Your request will be processed as soon as possible and within one month of receipt by us of such information that we may reasonably require to satisfy ourselves as to your identity and to locate the Information sought.

Please complete sections A-E, and return this form and proof of identity to BTG's Chair of the Committee (see Section D for details).

A. Your Details

Surname: **Forename(s)**

Male/Female **Former surname(s) (where relevant)**

Date of birth:

Address: This is the address to which all replies will be sent

Post Code: Country

Daytime telephone: Email:

Please indicate your relationship with BTG.

☐ Member ☐ Parent/Carer

☐ Service User ☐ Other

(specify below)

…….....

B Are you the Data Subject?

YES ☐

NO ☐

If you answered “Yes”, go straight to Section C. Otherwise, please provide the following information:

Surname: **Forename(s)**

Male/Female **Former surname(s) (where relevant)**

Address:

Post code: Email:

Daytime telephone:

Date of birth:

NOTE: If you are NOT the Data Subject, you must supply documentary evidence* to confirm the Data Subject’s authority which supports this request e.g. the Data Subject’s written authority, enduring power of attorney or the appointment of a Receiver by the Court of Protection.

* We must see certified copies - one on which a person able to sign (e.g. Justice of the Peace, solicitor, medical doctor) has certified that it is a true copy of the original document.

Section C

Data requested

Please describe the data which you are seeking as precisely as you can. Continue on a separate sheet if necessary:

Proof of Identity

Please enclose the following with this form:

Proof of your identity. Please supply a photocopy (not originals) of one of the following (if you cannot supply any of these items, please contact BTG).

- ☐ Full valid driving licence issued by a member state of the EU
- ☐ Birth certificate or certificate of registry of birth or adoption certificate
- ☐ Full valid current passport – only the identification page
- ☐ ID card issued by a member state of the EU
- ☐ Travel documents issued by the Home Office
- ☐ Certificate of Naturalisation or Registration

If the Data Subject's name is now different from that shown on the document you submit to confirm his/her identity, you must also supply documentary evidence to confirm the Data Subject's change of name e.g. marriage certificate, decree absolute or nisi papers, change of name deed or statutory declaration.

You must also confirm the address of the Data Subject by sending us a copy of one of the documents listed below. Please tick the appropriate box to indicate which document you have enclosed.

- ☐ Gas, electricity, water or telephone bill in the Data Subject's name for the last quarter
- ☐ Council tax demand in the Data Subject's name for the current financial year
- ☐ Bank, building society or credit card statement in the Data Subject's name for the last Quarter.

I confirm that I am either the Data Subject, or am acting on their behalf. I am aware that it is an offence to unlawfully obtain such personal data, e.g. by impersonating the Data Subject. I certify that I am the person named on this form and that I wish to be provided with the data which I have specified relating to myself under the Data Protection Act 1998, as updated by

the General Data Protection Regulation 2018. I will not publish any data which is supplied to me without prior permission from

I certify that the information given in this form is true. I understand that it is necessary for BTG to confirm my/the Data Subject's identity and it may be necessary to obtain more detailed information in order to confirm my identity and/or locate the correct information.

Signature: Print Name:

Please send your form and proof of identity to:

The British Toymakers Guild

Chair of the Committee
Email: info@toymakersguild.co.uk

Postal Address:

Numbers Limited
32 High Street
Wendover
Buckinghamshire
HP22 6EA

Data Protection Act Declaration

The data gathered by this form will be used to process your request for personal data under the Data Protection Act as updated by the General Data Protection Regulation. It will be held by the Chair of the Committee at BTG. The data will be held for six years from the date when we responded to your request, unless your request forms part of an ongoing case, in which case the data will be kept for as long as necessary.

.