BRITISH ASSOCIATION of DANGEROUS GOODS PROFESSIONALS

enquiries@badgp.org
www.badgp.org

Data Protection Policy

Key details

- Approved by BADGP Committee on: 1 December 2016
- Policy became operational on 3 December 2016
- Next review date: 1 December 2017

Introduction

The British Association of Dangerous Goods Professionals (hereafter "**BADGP**") is a non-profit organisation based in England.

BADGP needs to gather and use certain information about individuals.

These can include members, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the organisation's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures BADGP:

- Complies with data protection law and follows good practice
- Protects the rights of BADGP volunteers, staff, members and suppliers
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations — including BADGP— must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date

5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, Risks & Responsibilities

Policy scope

This policy applies to:

- The Administration Office of BADGP
- The members of the BADGP Committee, sub-groups and any other volunteers of BADGP
- All contractors, suppliers and other people working on behalf of BADGP

It applies to all data that the organisation holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus any other information relating to individuals

Data protection risks

This policy helps to protect BADGP from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how BADGP uses data relating to them.
- **Reputational damage**. For instance, BADGP could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with BADGP has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The members of the BADGP management Committee are ultimately responsible for ensuring that BADGP meets its legal obligations.
- The members of the BADGP management Committee are collectively and individually responsible for:
    - Keeping the Committee updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Handling data protection questions from anyone else covered by this policy.
    - Dealing with requests from individuals to see the data BADGP holds about them (also called ‘subject access requests’).

- Checking and approving any contracts or agreements with third parties that may handle BADGP's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Evaluating any third-party services that BADGP is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within BADGP or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Data Storage

These rules describe how and where data should be safely stored.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. The central stores of data for BADGP are the online Wild Apricot Membership and Event Management system.

The Security Policy of the Wild Apricot Membership and Event Management system can be viewed at: http://www.wildapricot.com/security-policy-overview.

In addition:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.

- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

Personal data is of no value to BADGP unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Ideally, data should be encrypted before being transferred electronically. The Wild Apricot Membership System has been configured so that all data transfers are encrypted by use of SSL.
- Personal data should never be transferred outside of the European Economic Area.

Data Accuracy

The law requires BADGP to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort BADGP should put into ensuring its accuracy. BADGP make members' and contacts' data available to them, online, through their own User Profile, so that they can help ensure accuracy of the data held.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- BADGP will continue to make it easy for data subjects to update the information BADGP holds about them. This can be done by the data subjects accessing, checking and editing their own data via the Wild Apricot Membership system.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests

All individuals who are the subject of personal data held by BADGP are entitled to:

- Ask what information the organisation holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the organisation is meeting its data protection obligations.

If an individual contacts BADGP requesting this information, this is called a "subject access request".

Subject access requests from individuals should be made by email, to enquiries@badgp.org. We will aim to provide the relevant data within 14 days.

We will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data For Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, BADGP will disclose requested data. However, we will ensure the request is legitimate, seeking assistance from the BADGP management Committee and from the organisation's legal advisers where necessary.

Providing information

BADGP aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, BADGP has a privacy statement, setting out how data relating to individuals is used by the Association. This can be viewed by visiting: http://www.badgp.org/resources/badgp-privacy-policy-version-1-dec-2016.pdf .