BFAWU Data Protection Policies for Representatives

BFAWU Data Protection for Representatives

All representatives of the BFAWU will handle personal data of other individuals in their capacity as a representative. It is therefore essential that representatives are aware of the rights of the individuals whose data they are handing (referred to as “data subjects”) and their obligations when doing so. As “Data Controller”, the BFAWU is responsible for those handling data on its behalf.

BFAWU Membership Privacy Policy

The BFAWU have a Membership Privacy policy which is available on their website or can be provided in printed form, where requested. This identifies the data that the BFAWU may handle and its reasons for doing so.

Data protection legislation

The General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018defines how your personal information is used by organisations, businesses or the government. Everyone responsible for using personal data has to follow strict rules called ‘data protection principles’. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people’s data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

Personal Data

Personal data is any information held about living, identifiable people such as:

- Their address (either work, home or other)
- Their contact details (email, phone number etc…)
- Their NI number
- Their employment details (where they work, payroll number etc…) (and including anything relating to issues at work such as disciplinary, accidents etc..)
- Their bank account details
- Any statement they have provided or in which they have been named
- Medical records (sick certificates, medical reports etc…)

Data Security

When handling personal data, consider the following tips:

- Don’t leave PCs unattended when logged on
- Keep passwords safe and don’t disclose it to anyone
- If working on PC on personal data make sure no-one who might be in the vicinity can see it
- Avoid use of removable media (memory sticks etc…) for storing personal data as far as possible. If entirely necessary, ensure it has encryption in place

- Remember that email is not a secure medium for sending confidential information.
- File titles should not be worded so that they contain personal information (don't include address for instance)
- Paper records containing personal data should be stored in a secure environment i.e. locked cupboards/cabinets whenever unattended
- Mail containing confidential information not sent to the addressee's private address should be clearly marked "Private & Confidential; for the Addressee Only"
- Any paper records to be disposed of should be done so securely if they contain confidential/personal information
- Care should be taken when discussing confidential information in the presence of others
- Information should not be disclosed to anyone other than the subject of that information unless prior consent has been given

Data Subject Rights Procedure

The BFAWU operates a Data Subject Rights Procedure that all representatives should familiarise themselves with. This Procedure should be referred to whenever a data subject wishes to exercise their rights as identified in the procedure.

Data Breach Procedure

The BFAWU operates a Personal Data Breach Procedure that all representatives should familiarise themselves with. It should be borne in mind that there is only a short period of time within which the BFAWU should react to any potential Breach and it is therefore essential that the Procedure is adhered to as soon as possible after and potential breach has been identified.

Conclusion

Data protection affects all of us. As stated above, it is essential that anyone handling data on behalf of the BFAWU does so in accordance with the BFAWU policies. If you are unsure as to how to proceed when doing so, please ask before acting: either locally via your Full Time Official or email the BFAWU Data Protection Lead at: dpa@bfawu.org

BFAWU membership privacy policy

Who we are

The Bakers Food and Allied Workers Union (BFAWU) is the largest independent Trade Union in the food sector in the British Isles. First established in 1847, we have over 175 years of experience in representing employees in the food sector, from production at factories through to sales at shops. We are run by our members for our members, with a fully elected governing body who are answerable to our membership.

We are registered with the Information Commissioner's Office and our registration number is Z8988634. Our office headquarters is based at: Stanborough House, Great North Road, Stanborough, Welwyn Garden City, Hertfordshire. AL8 7TA.

Our Data Protection Lead is our General Secretary, contactable at: dpa@bfawu.org

What personal data we collect

To fulfil our aims as a trade union, we need to collect and use personal data relating to our members. This will include:

- Name
- Address and other contact details
- Date of birth
- Employer
- NI number
- Bank account details (if paying by direct debit)
- Gender
- Ethnicity (where you choose to provide it)
- Membership payment records
- Mailing preferences
- Photographs (if taken at events)
- Health/disability information (if relevant to an issue we are supporting you with e.g. sickness benefit)
- Grant fund applications (if applying for a grant)

Why we use your personal data

Data protection legislation requires us to have a lawful basis in place for our use of personal data. Our lawful bases and related purposes are set out below.

We have a **legal obligation** to:

- Run ballots to elect executive council
- Run ballots to elect national officers
- Maintaining our electoral roll
- Run industrial action ballots
- Meet our health and safety compliance obligations, to staff, volunteers and attendees at events
- Assess and appoint new trustees e.g. information required by the Charity Commission
- Publish our annual report and accounts
- Meeting Trade Union Act and other legal obligations (e.g. HMRC and AML) audit trail obligations such as tax, donations from members.
- Meet Trade Union Act obligations for the recording on membership information
- Identify picketing supervisors, as required by the Trade Union Act

We have **contractual obligations** to:

- To provide you with the services set out in the union rulebook

We have a **legitimate interest** to:

- Run ballots to elect full time officers
- Record attendance at conference and regional councils
- Run other ballots (e.g.: Branch elections)
- Record and circulate minutes relating to official meetings
- Administer our annual conference
- Record and process membership contributions via wages
- Check expense claims and prevent fraud
- Deal with complaints from members
- Ensure fair representation and opportunity within the union
- Send surveys relating to the work and aims of the union
- Take photos at events and use for publicity purposes (can object to use)

We will ask you for your **consent** to:

- Send you direct marketing messages by email or SMS
- Publish case studies where we have represented and helped our members

You can withdraw your consent at any time by contacting us at dpa@bfawu.org

Special category data

As trade union membership constitutes special category data under data protection legislation, we will also rely on Article 9(2)(d) of GDPR to use personal data in line with BFAWU's legitimate activities as a trade union aim. This on condition that the processing relates solely to our members or former members and that the personal data are not disclosed outside BFAWU without your consent.

Who we share your personal data with

We employ the services of certain third parties to deliver services on our behalf, as below:

- Unity e-Payments (for financial transactions)
- Unity Trust Bank (facilitate the above transactions)
- Bacs (to facilitate direct debits)
- Plastic Card Services (to issue membership cards)
- Computing Information Services (CIS) (BFAWU IT support)
- Access (to provide our CRM and accounting software)
- Electoral Reform Services (to run our elections/ballots)
- Solicitors (where legal advice/support is required)
- Auditors

Your rights

Under data protection legislation,

- The right **to be informed** about processing of your personal data (as per this policy)
- The right to have your personal data **corrected** in case of inaccuracy and to have incomplete personal information completed.
- The right to **object** to processing of your personal data.
- The right to **restrict** processing of your personal data.
- The right to **erasure** of your personal data.

- The right to **request access** to your personal data and information about how we process it.
- The right to **move** your personal data (Data Portability).
- The right to **withdraw consent** (where use of personal information is based on consent)

These rights are not absolute and may not apply in all circumstances, depending on our reason for using your personal data. For further information in relation to these rights, please see the Information Commissioner's Office website.

If you wish to exercise any of the rights set out above, please contact us by writing to us at: BFAWU Head Office, Stanborough House, Great North Road, Welwyn Garden City, Herts AL8 7TA or dpa@bfawu.org We may take steps to verify your identity before processing a request.

How long we keep your personal data

We will retain your personal data during your period of membership and for a defined period once your membership ends. We are required to keep certain information relating to financial transactions for statutory periods (usually six or seven years).

Review

This policy will be reviewed at least annually. We will communicate any updates to our members once approved.

BFAWU Personal Data Breach Procedure for Representatives

Introduction

This document sets out BFAWU's procedure in relation to reporting and managing breaches involving personal data. It applies to all BFAWU staff, agency workers, volunteers, contractors and third party agents who process data for or on behalf of BFAWU and it must be complied with in the event of a personal data breach.

Definition of personal data breach

A personal data breach is defined within Article 4 of GDPR as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, theft, or unauthorised access, to personal data."

Breaches can include a number of different scenarios and some (non-exhaustive) examples include:

- Loss or theft of personal data or equipment (encrypted and non-encrypted devices) on which personal data is stored, e.g. loss of paper record, laptop, tablet or USB stick
- Inappropriate access controls allowing unauthorised use, e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to personal data or information systems
- Email containing personal data sent to the incorrect recipient
- Unauthorised disclosure of sensitive or confidential information, e.g. document posted to an incorrect address or addressee
- Unforeseen circumstances such as a fire or flood
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it
- Insecure disposal of paperwork containing personal data

Internal reporting

Serious personal data breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours of detection, and without undue delay to individuals affected by the incident. Therefore, it is vital that all staff and volunteers report a personal data breach, or suspected personal data breach, however minor, as soon as possible after discovery so that it can be managed and investigated.

The primary point of contact for reporting a data breach incident is the Data Protection Lead, dpa@bfawu.org. As soon as is practicably possible, please contact your Regional Office who will obtain from you the information necessary to report the incident(s) to them.

The Data Protection Lead (or nominated deputy) will then investigate the breach to assess the level of risk to the individual(s) concerned, the necessary follow up actions to be taken and whether any further notification is required (see below). The follow up actions required will be dependent on the context and cause of the breach.

Assessment of breach and whether it is reportable

A personal data breach is reportable to the Information Commissioner's Office (ICO) where it is likely to result in a risk to the rights and freedoms of the individual(s) concerned. The decision whether to report a breach is not a scientific one and, when assessing the risks, must take into account all the factors and context relating to the breach, including:

- The type of breach
- The nature and sensitivity of personal data
- The number of affected individuals
- The ease of identification of individuals
- The severity of consequences for the individuals
- Any special characteristics of those affected
- Any evidence that individuals have been affected by the breach

The Data Protection Lead or nominated deputy will make an assessment of whether a personal data breach is reportable.

Breach reporting – to the Information Commissioner's Office (ICO)

The Data Protection Lead or nominated deputy will notify the ICO, without undue delay, of a reportable personal data breach and include a description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the Data Protection Lead or main point of contact;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Breaches can be reported directly via the ICO's website at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

Breach notification - data subject

Where the personal data breach, or suspected personal data breach, is likely to have an impact on the rights and freedoms of the data subject, BFAWU shall notify the affected data subjects, without undue delay, in accordance with the Data Protection Lead's recommendations.

Enforcement

Failure to adhere to this procedure, delay in reporting the breach to the Data Protection Lead and non-reporting of breaches, may result in further action.

Record keeping

The Data Protection Lead will keep a record of all personal data breaches, whether considered reportable to the ICO or not). Understanding the cause of breaches and any recurring trends allows us to develop and implement systems and processes that are more robust to prevent future breaches and protect personal data.

Review

This procedure will be reviewed annually or where significant changes have occurred.

BFAWU Data Subject Rights Procedure

1. Introduction
The General Data Protection Regulation (GDPR) creates some new Rights for Data Subjects
as well as strengthening existing Rights. As a Data Controller, the BFAWU must be able to comply with these Rights. The GDPR provides the following Rights for individuals:

- Right of **Access** (Also known as a Subject Access Request)
- Right to **Rectification**
- Right to **Erasure**
- Right to **Restrict Processing**
- Right to **Data Portability**
- Right to **Object**
- Rights in **Relation to Automatic Decision Making and Profiling**

These rights are not absolute and they are dependent upon the lawful basis we are relying on for a particular type of processing.

2. Scope and recognition of requests
It is important to recognise that such requests may be made by current or past BFAWU members, staff, volunteers or any other individual about whom BFAWU holds personal data and can be received by any member of BFAWU staff or representative. Such request may not follow a clear and standard format where the requester clearly sets out which right they are requesting to be exercised. For example, a person may simply say *'I want to know what the BFAWU is using my data for'* or *'I want to see all emails about me in the BFAWU system'*.

It should be noted that people can make such requests verbally (for example, over the telephone), as well as in an email or postal letter.

3. Responsibilities
All staff and representatives have a responsibility to recognise a request and to comply with the
procedure as follows. As there is legal time limit ("one month") within which requests must be responded to, it is vital staff and representatives recognise such requests and pass them on as soon as possible.

4. Verification of identity
Where appropriate, we will make checks to enable us to verify the identity of the requester. Such verification will depend on the nature and context in which the relevant personal data is held. We must also consider what information we can genuinely verify against and ensure we are not processing personal data in an excessive manner.

5. Time limit for response
As above, requests must be responded to without undue delay and within "one month". This time period starts once we have verified the identity of the requester (where we choose to do so). Consequently, all Subject Access requests must be passed to the Data Protection Lead: dpa@bfawu.org within two weeks of the request being received. (see 6. Below).

6. Procedure
Where a request is received by staff or representatives covering any of the Data Subject Rights set out in section 1, the request must be forwarded tot the Data Protection Lead,

using the form Appendix 1 below, to: dpa@bfawu.org with the subject heading “Data Subject Rights Request” within two weeks of the request being received.to make an assessment about the action required.

The request will be processed accordingly by the Data Protection Lead or their nominated deputy and responded to in line with the legislation. They may ask for input and/or provision of data from teams across the BFAWU in order to ensure they have fully complied with the request. Due to the time limits for complying, and potential penalties for non-compliance, teams requested to assist should treat such requests as a priority.

- **Exception to the above - Updating records**
  For routine requests to update personal data (e.g. change of address), while technically rectification requests, these can be processed without referral to central BFAWU office.

7. “Manifestly unreasonable” requests
Where a request is considered to be “manifestly unfounded or excessive”, in particular because of their repetitive character, we may either:

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- refuse to act on the request.

There are no set guidelines about when a request or requests may fall into this category but a decision will be taken by the Data Protection Lead, taking into account all the relevant context in relation to the request(s).

8. Record keeping
The Data Protection Lead will maintain a record of all data subject rights requests to ensure they have been dealt with within the timescales set out in the legislation and to provide evidence of our data protection compliance.

Appendix 1 - Data Data Subject Rights Reporting Form

Instructions: This form is to be completed as soon as possible following receipt of a data subject request. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

1. Subject Details	
Name:	
Membership Number	
Branch	
Work Phone:	
Mobile Phone:	
Email address:	

2. Request Details.
☐ Right of Access (Also known as a Subject Access Request) ☐ Right to Rectification ☐ Right to Erasure ☐ Right to Restrict Processing ☐ Right to Data Portability ☐ Right to Object ☐ Rights in Relation to Automatic Decision Making and Profiling
☐ Time and date request received:
Provide a brief description of what has been requested:

3. Request Method
☐ Telephone ☐ Letter ☐ Email
5. Details Taken By:

Name	
Position	
Date	

Please submit this completed form to: dpa@bfawu.org with the Subject Heading “Data Subject Rights Request”

BFAWU Clear Desk Policy

Clear Desk
All documents that contain any personal information should not be left on desks unattended and should be removed from view when unsupervised.

All documents should be collected from printers as soon as they are produced – and not left where they can be read by passers by.

At the end of each day, all documents that contain any personal information must be:

- cleared from every desk,
- cleared from trays or other 'inboxes' (or the trays themselves moved to a secure locations),
- cleared from printers, photocopiers or fax machines, and
- stored in a locked cupboard, cabinet, set of draws or safe overnight.

All other information may be left on desks in a tidy manner.

Clear Screen
Users must ensure that any PC, laptop or other device they are using that is left unattended is locked or logged out to prevent unauthorised access.

- Screens will be set by ICT to lock automatically a period of inactivity, and a screen saver with password protection will be enabled on all devices.
- Attempts to tamper with this security feature will be investigated and may be subject to action.

Users must leave nothing on display that may contain access information, such as login names or passwords.

Users are responsible for safeguarding personal information on their device by ensuring that the device is not left logged-on when unattended, and that portable devices in their custody are not exposed to opportunistic theft.

Removing Data & Offsite Working
There should not be a need to remove data from your workplace. If, however, this does occur, then care should be taken with what is removed should be Locked away and kept out of sight when left unattended, and not left where it would attract the interests of the opportunist thief:

- **At home**: this means located out of sight of the casual visitor, family members or others who share your accommodation. Ideally any home office area should be separate from the rest of the house.
- **In transit:** Concealed when being transported.and not being left unattended for any period of time, including when visiting the toilet, buying refreshments, or otherwise being away from the information or device.

Waste
Users must ensure all waste paper is handled according to its classification / sensitivity, using the shredding facilities provided.

BFAWU Data Protection and GDPR Advice for Representatnvies

Data Protection advice given to: _____ *(Name)*

Of Branch: _____ *(Branch No.)*

Date: _____

Delivered by: _____ *(FTO)*

I confirm that I have been advised of my responsibilites under DPA & GDPR and am aware of the same:

Signed: _____ *(BFAWU Rep)*

Date: _____

Completed Form to be sent to Regional Office