Department	**BPIF Training**
Reference	**P0028**
Title	**Data Protection Policy**
Version	**4**
Issue Date	**1st December 2021**
Review Date	**1st December 2022**
Original Issue Date	**9th October 2016**

Data Protection Policy

PURPOSE

BPIF Training is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the BPIF's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, interns, apprentices and former employees, referred to as HR-related personal data.

This policy does not apply to the personal data of clients or other personal data processed for business purposes.

The BPIF has appointed Charles Jarrold, CEO, as the person with responsibility for data protection compliance within the BPIF. They can be contacted at Charles.jarrold@bpif.org.uk. Questions about this policy, or requests for further information, should be directed to him.

DEFINITIONS

“The BPIF” refers to BPIF Unincorporated, BPIF Limited, and BPIF Training Ltd

"Personal data" is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

DATA PROTECTION PRINCIPLES

The BPIF processes HR-related personal data in accordance with the following data protection principles:

- The BPIF processes personal data lawfully, fairly and in a transparent manner.
- The BPIF collects personal data only for specified, explicit and legitimate purposes.
- The BPIF processes personal data only where it is adequate, relevant and limited to what is necesssary for the purposes of processing.
- The BPIF keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The BPIF keeps personal data only for the period necessary for processing.
- The BPIF adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The BPIF tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where the BPIF processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

The BPIF will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor or apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the BPIF holds HR-related personal data are contained in its privacy notices to individuals.

The BPIF keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

In order to comply with the Data Protection Act 2018 BPIF will process candidate's personal data in accordance with the data protection principles, namely:

1. Personal data shall be processed fairly, lawfully and transparently.
2. Personal data shall be obtained only for candidate registration purposes and shall not be further processed in any manner incompatible with that.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for candidate registration shall not be kept for longer than is necessary.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Purposes for which Personal Data may be held

Personal data relating to employees may be collected primarily for the purposes of

- Recruitment, promotion, training, redeployment and/or career development;
- Administration and payment of wages;
- Calculation of certain benefits including pensions;
- Disciplinary or performance management purposes;
- Performance review;
- Recording of communication with employees and their representatives;
- Compliance with legislation;
- Provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and
- Staffing levels and career planning.

BPIF considers that the following personal data falls within the categories set out above:

- Personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant;
- References and CVs;
- Emergency contact details;

- Notes on discussions between management and the employee;
- Appraisals and documents relating to grievance, discipline, promotion, demotion or termination of employment;
- Training records;
- Salary, benefits and bank/building society details; and
- Absence and sickness information.

BPIF will review the nature of the information being collected and held on an annual basis to ensure there is a sound business reason for requiring the information to be retained.

Sensitive Personal Data
Sensitive personal data includes information relating to the following matters:

- The employee's racial or ethnic origin;
- His or her political opinions;
- His or her religious or similar beliefs;
- His or her trade union membership;
- His or her physical or mental health or condition;
- His or her sex life; or
- The commission or alleged commission of any offence by the employee.

To hold sensitive personal data, the Company must additionally satisfy a sensitive data condition. The most appropriate condition for employment purposes is that the processing is necessary to enable BPIF to meet its legal obligations (for example, to ensure health and safety or to avoid unlawful discrimination).

Responsibility for the Processing of Personal Data

The compliance team are responsible for ensuring all personal data is controlled in compliance with the Data Protection Act 2018.

Employees who have access to personal data must comply with this Policy and adhere to the procedures laid down by the Data Controller. Failure to comply with the Policy and procedures may result in disciplinary action up to and including summary dismissal.

Use of Personal Data

To ensure compliance with the Data Protection Act 2018 and in the interests of privacy, employee confidence and good employee relations, the disclosure and use of information held by the Company is governed by the following conditions:

- Personal data must only be used for one or more of the purposes specified in this Policy;
- Company documents may only be used in accordance with the statement within each document stating its intended use; and
- Provided that the identification of individual employees is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data (e.g., surveys, staffing level figures); and
- Personal data must not be disclosed, either within or outside the Company, to any unauthorised recipient.

Personal Data Held for Equal Opportunities Monitoring Purposes

Where personal data obtained about candidates is to be held for the purpose of equal opportunities monitoring, all such data must be made anonymous.

Disclosure of Personal Data

Personal data may only be disclosed outside the Company with the employee's written consent, unless disclosure is required by law or where there is immediate danger to the employee's health.

Accuracy of Personal Data

The Company will review personal data regularly to ensure that it is accurate, relevant and up to date.

In order to ensure the BPIF's files are accurate and up to date, and so that BPIF is able to contact the employee or, in the case of an emergency, another designated person, employees must notify the Company as soon as possible of any change in their personal details (e.g., change of name, address; telephone number; loss of driving licence where relevant; next of kin details, etc).

Personnel update forms will be issued to all employees on an annual basis for the purposes of ensuring the data is up to date and accurate. Employees will be entitled to amend any incorrect details and these corrections will be made to all files held on BPIF's information systems. In some cases, documentary evidence, e.g., qualification certificates, will be requested before any changes are made. Once completed, these records will be stored in the employee's personnel file.

INDIVIDUAL RIGHTS

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the BPIF will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the BPIF has failed to comply with their data protection rights; and
- whether or not the BPIF carries out automated decision-making and the logic involved in any such decision-making.

The BPIF will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

To make a subject access request, the individual should send the request to anna.stretton@bpif.org.uk. In some cases, the BPIF may need to ask for proof of identification before the request can be processed. The BPIF will inform the individual if it needs to verify their identity and the documents it requires.

The BPIF will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the BPIF processes large amounts of the individual's data, it may respond within three months of the date the request is received. The BPIF will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the BPIF is not obliged to comply with it. Alternatively, the BPIF can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the BPIF has already responded. If an individual submits a request that is unfounded or excessive, the BPIF will notify him/her that this is the case and whether or not it will respond to it.

OTHER RIGHTS

Individuals have a number of other rights in relation to their personal data. They can require the BPIF to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the BPIF's legitimate grounds for processing data (where the BPIF relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the BPIF's legitimate grounds for processing data.

To ask the BPIF to take any of these steps, the individual should send the request to anna.stretton@bpif.org.uk.

DATA SECURITY

The BPIF takes the security of HR-related personal data seriously. The BPIF has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the BPIF engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

DATA BREACHES

If the BPIF discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The BPIF will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

INDIVIDUAL RESPONSIBILITIES

Individuals are responsible for helping the BPIF keep their personal data up to date. Individuals should let the BPIF know if data provided to the BPIF changes, for example if an individual moves house or changes their bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, internship or apprenticeship. Where this is the case, the BPIF relies on individuals to help meet its data protection obligations to staff [and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;

- not to disclose data except to individuals (whether inside or outside the BPIF) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the BPIF's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the BPIF's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

TRAINING

The BPIF will provide training to all individuals about their data protection responsibilities as part of the induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

REVIEW

The Data Protection Policy was updated on 1st December 2021. The policy is to be reviewed annually, as a minimum with the next review date being no later than 1st December 2022.