16th October 2023

General Data Protection Regulation (GDPR) Policy

Introduction

We hold personal data about our employees, members, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff/members understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff/members to ensure that the Data Protection Officer (DPO)(Presidium of the Board) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

What is GDPR?

Keeping information about clients and staff/members confidential makes clear business sense but it is also required by law. The EU General Data Protection Regulation (GDPR) defines the ethical handling of personal data. Replacing legislation written before the digital age, the regulation became EU law in 2016, enforceable from 25th May, 2018.

Definitions

Business purposes

The purposes for which personal data may be used by us:
Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- *Compliance with our legal, regulatory and corporate governance obligations and good practice*
- *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests*
- *Ensuring business policies are adhered to (such as policies covering email and internet use)*
- *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of Personal data, Sensitive personal data, Data Controller, Data Processor, Processing commercially sensitive information, security vetting, credit scoring and checking*
- *Investigating complaints*
- *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments*
- *Monitoring staff/member conduct, disciplinary matters*
- *Marketing our business*
- *Improving services*

Information relating to identifiable individuals, such as job applicants, current and former employees, agency, members, Directors, contractors and other staff, clients, suppliers and marketing contacts.

Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy. This can include subcontractors and agents. Processors must maintain records of personal data and processing activities and will have legal liability if responsible for a breach.

An organisation that determines the way in which personal data is processed. The controller must be able to demonstrate compliance with the principles and ensure contracts with data processors comply with the GDPR. Company secretary or accountant.

Collecting, disclosing, storing, using or any other operation performed upon personal data. If you use personal data in any way you will be "processing" it.

Scope

This policy applies to all staff/members.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff/members before being adopted.

Who is responsible for this policy?

Board Presidium has overall responsibility for the day-to-day implementation of this policy.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Board of Directors are:

- To be kept updated about data protection responsibilities, risks and issues
- The reviewing of all data protection procedures and policies on a regular basis
- Arrangement of data protection training and advice for all staff members and those included in this policy
- The Answering of questions on data protection from staff, board members and other stakeholders
- Responses to individuals such as clients and employees who wish to know which data is being held.
- The Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Responsibilities of the IT Services (third party)

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services BDC considering using to store or process data.

Responsibilities of the Accountant (third party)

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and BDC Data Protection Policies.

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice to clients on data protection. The notice:

- Sets out the purposes for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as other professional advisers
- Provides that customers have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the BDC Office so that they can update your records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the BDC office will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- We do not store data on memory sticks
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure non-international location.
- Data should be regularly backed up in line with the company's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Data Protection Officer.

Subject access requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If a subject access request is received, it should be referred to the DPO.

Please contact the BDC Office if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

What information is being collected?

Who is collecting it?
Our members, suppliers & employee's data is collected as and when a new one arises.
Data used for mailing purposes are supplied by our clients to be processed according to the completed application of membership/work.

How is it collected?
Our member, supplier & employee's data is collected at the initial stage when receiving membership applications. Information will be collected via email & post to satisfy the needs of our documentation.

Why is it being collected?
We are provided data by our members to process licenses and memberships. Third parties are informed of data if consent is given.
We collect information on our suppliers to conduct business and provide invoices.

We collect information on employees to pay them their wages & provide their tax information to HMRC.

Who will it be shared with?
Data may be shared with a third party supplier if it is deemed appropriate with member consent.
We also may share the data externally if exceptional circumstances apply or we are required to do this by law.

Justification for personal data

We will process personal data in compliance with all eight data protection principles:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful & legitimate purpose
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

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time. With reference to the data supplied by our members/customers to conduct a job, it is our customers responsibility as the data owners to gain active consent.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA. This consent may be actioned by the BDC Office.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary – Non-conformance Report
- Maintain a register of compliance failures – Non-conformance Log
- Notify the Supervisory Authority (ICO – Information Commissioner's Office) of any compliance failures that are material either in their own right or as part of a pattern of failures

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts the organisation at risk.