European Asbestos Services

Data Protection Policy

Introduction

European asbestos services have a requirement to gather, hold and use certain information about individuals.

These will include employees, suppliers, professional organisations, business contacts, customers and other people that the business has a relationship with or would be require to or have a need to contact.

This policy clearly describes the how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply to the law, regulation and best practice.

What this policy covers

This policy details your rights and obligations in relation to your personal data and the personal data of third parties that you may come into contact with during the course of your employment. If you have access to the personal data of employees or of third parties, you must comply with this policy. Failure to comply with the Policy and procedures may result in disciplinary action up to and including dismissal without notice.

Why this policy exists

This policy has been created to ensure that the European asbestos services: -

- Meets its obligation under the data protection act and the general data protections regulations
- Upholds the rights of its staff, customers, interested parties, stakeholders and others
- Is transparent in the way it collects, process and stores this information
- Sets out the controls that protect against a data loss or breach

Data Protection law

This law sets out the how European asbestos services is allowed to collect, handle, store and use personal information.
And the rules apply if the information is stored electronically, on paper or other material.

The overriding requirement is that personal information that must be collected is used fairly, stored securely and safely and not disclosed unlawfully to others

Data protection is governed by eight principles and are as follows: -

- Data must be processed fairly and lawfully
- Data must be obtained for a specific, lawful purpose
- Data must be adequate, relevant and not excessive
- Data must be accurate and kept up to date
- Data cannot be held for any longer than necessary
- Data must be processed in accordance with the rights of the data subject
- Data must be protected in appropriate ways
- Data must not be transferred outside of the European Economic Area (EEA), unless the country or territory also ensures an adequate level of protection

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018.
The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

General Data Protection Regulation is governed by seven principles and are as follows: -

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Data Protection Policy Scope

The data protection policy applies to: -

- The Head Office
- All Branch and Regional Offices
- All Staff and Volunteers
- All contractors, sub-contractors, suppliers and others working on behalf of European asbestos services

The data protection policy applies to all data that the company hold relating to identifiable individuals, even if that information technically falls outside of the data protection act 1998. This will include:-

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

Data Protection Risk

The data protection policy helps to protect European asbestos services from some of the associated risk regarding personal data: -

- **Breaches of confidentiality**. For examples information being given out inappropriately.
- **Failing to offer a choice**. All individuals should be free to choose how the company uses data that relates to them.

- **Reputational damage**. If the company suffered a cyber-attacker or hackers gained access to information.
- **Fines for failing to meet the requirements.** Not registering with the ICO is a criminal offences and data breaches and loss can incur fines of up to £20 Million or 4% of turnover.

Responsibilities

Everyone who works for or on behalf of or with European asbestos services has some responsibilities for the data that is collect, handle, store and used.

Everyone that handles personal data must ensure that it is done so in accordance with this policy and in line with the eight principles of data protection.

The following people have key responsibilities and they are as follows: -

The board of directors is ultimately responsible for ensuring that the European asbestos services meets it legal obligation.

The data protection officer, is Arzu Hassan and they are responsible for: -

- Keeping the board updated about data protection issues, risks and responsibilities
- Reviewing all data protection procedures and policies in a timely manner.
- Arranging and providing data protection training and advice for people covered by this policy
- Dealing with requested from individuals to see the data the company hold on them (aka subject access requests)
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The operations director will be responsible for: -

- Ensuring that all systems and equipment, electronic or other used for the storage of data meets the security standards.
- Will conduct or arrange for performance checks and scans to ensure that security hardware and software is functioning properly.
- Conduct an evaluation of any third parties the company uses or is considering using for the storage or processing of its data for example cloud computing services/ propeller studios. The marketing/ bid team manager will be responsible for: -

- Approving any data protection statements attached to emails and letters.
- Addressing any data protection queries from external sources e.g. media and journalist's outlets.

- And work with other staff to ensure that marking initiatives abide by the data protection principles.

Staff Guidelines

Are as follows: -

- The only people able to access data coved by this policy are those who need it for their work.
- No data should be shared informally between staff and confidential information should be provided only by managerial approval.
- Training will be provided to all employees to help with their understanding and responsibilities.
- Data must be kept secure by taking sensible precautions to prevent its loss, corruption or theft.
- Access passwords must be strong and never shared.
- Data must not be disclosed without permission either within the company or with external parties.
- Data must be regularly reviewed and updated, if found to be out of date or no longer required, it should be deleted shredded and disposed of.
- Employees should request help from the DPO data protection officer if they are unsure of any aspect of data protection.

Storage of data

Are as follows for paper records: -

- When not required, the records or files should be kept in a locked drawer or filling cabinet. Paper records or printouts are not left where unauthorised people could see them or gain access to them like on the printer.
- Paper records and printouts should be shredded and disposed of securely when no longer required.

For electronically stored records: -

- Data must be kept secure and protected by passwords and these are changed regularly and never shared.
- Data stared on removable items i.e. CD, DVD Memory sticks and external hard drives, these should be kept locked away securely when not in use.
- Data must only be stored on designated drives and servers and should only be uploaded to a secure and approved cloud storage provider.

- Servers that contain personal data will need to be stores away from general office space. Data should be backed up frequently and those backups tested to ensure that data is not lost.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All computers and servers should be protected by suitable security software and firewall.

Using stored data

Personal data doesn't provide a value unless the business 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 that screen of their computers are always locked when left unattended.
- Personal data should not be shared informally, it should not be sent via email as this form of communication is not secure.
- Data that is being transferred must be encrypted, (the Easybop system is encrypted at source and meets the requirements of ISO27001)
- Personal data cannot be transferred outside of the European economic area (EEA)
- Personal data should not be saved onto personal computers or removable storage devices.

Accuracy of stored data

The data protection act requires European asbestos services to take reasonable steps to ensure that the data it holds is accurate and up to date as far as reasonably practicable: -

- Data should be held in as few places as necessary, with staff not creating any unnecessary data sets.
- Staff should take every opportunity to ensure that data held is accurate by confirming details with the data subject.
- Availability for easy access to the data should be available for the subject to update their own information.
- Personal data should be updated as any inaccuracies are discovered.
- Marketing information need to be reviewed and updated every six months by the marketing and bid team manager.

Subject access requests

All individuals that have personal information held by European Asbestos Services are entitled to:-

- Ask what information the company hold about them and why it is held.
- Ask how they can access this information.

- Be informed of how they can keep it up to date.
- Be informed hoe the company is meeting the data protection obligations.

Should an individual contact the company requesting this information this is known as a subject access request.

Subject access request should be made in righting or email to the data protection officer. Individuals requesting the subject access request will be charged £10.00 per subject access request, and the data protection officer will need to respond within 40 days once payment has been received.

The data protection officer will always verify the identity of anyone making a subject access request before disclosing any information.

Disclosure of data for other reasons

There are certain circumstances that allows for the disclosure of personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances European asbestos services will disclose requested data, however the data protection officer will ensure that the request is legitimate, seeking assistance from the board and from the company legal adviser where necessary.

Your information

Personal Data means data held either on a computer or in a paper-based filing system which relates to a living individual who can be identified from that data.

The Data Protection Act 1998 prescribes the way in which the Company may collect, retain and handle personal data. The Company will comply with the requirements of the Data Protection Act and all employees and contractors who handle personal data in the course of their work must also comply with it.

<u>The purposes for which your personal data may be held by the Company</u>

Personal data relating to employees may be collected by the Company for the purpose of:-

- Recruitment, promotion, training, redeployment and / or career development, such as references, CVs and appraisal documents
- Administration and payment of wages, such as emergency contact details and bank/building society details
- Calculation of certain benefits including issues
- Disciplinary or grievance issues
- Performance management purposes and performance review
- Recording Management purposes and performance review
- Recording of communication with employees and their representatives

- Compliance with legislation
- Provision of references to finical institutions, to facilitate entry onto educational courses and/or to assist future potential employers and
- Staffing levels and career planning

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

- Your racial or ethnic origin
- Your political opinions
- Your religious or similar beliefs
- Your trade union membership
- Your physical or mental health condition
- You sex or sexual orientation
- The commission or alleged commission of any offence by you

Personal data relating to non-employees or external organisations and businesses may be collected by the Company for the purpose of:

- Contact details for the arranging of appointments, meeting and attendance for works.
- Administration of invoicing and payment of invoices, including bank/building society details
- Calculation of information between interested parties (health and safety guidance etc.)
- Marketing and evaluation of performance surveys
- Compliance with legislation

Procedure

Processing of sensitive data

The Company will process sensitive data primarily where it is necessary to enable the Company to meet its legal obligations and in particular to ensure adherence to health and safety and vulnerable groups protection legislation or for equal opportunities monitoring purposes. In most cases, the Company will not process sensitive personal data without your consent.

Accuracy of personal data

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

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

Security of personal data

The Company will ensure that personal data is not processed unlawfully, lost or damaged. If you have access to personal data during the course of your employment, you must also comply with this obligation. If you believe you have lost any personal data in the course of your work, you must report it to the data protection officer immediately. Failure to do so may result in disciplinary action up to and including dismissal without notice.

Mr Gary Spillane
Managing Director

Review 28 February 2021