GDPR DATA PROTECTION POLICY

Context and overview Key details;
Policy prepared by: Katrina Davey-Reid - Recruitment Team, Training and Support Manager 16/10/19
Reviewed by; Hannah Lomotey Marketing Manager and Administration Manager 31/12/17 Approved by: Colin Smith - Director on 31/12/17
Policy became operational on: 01/01/2018
Next review date: 16/10/2020

Introduction AES needs to gather and use certain information in our capacity as a recruitment business. This data can come from customers, 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 company's data protection standards and to comply with the law.

Why this policy exists This data protection policy ensures AES:

- Complies with data protection law and follow good practice.
- Protects the rights of staff, customers, suppliers and licence holders of AES.
- 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 AES, 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 and responsibilities Policy scope; This policy applies to:

- The head office of AES
- All staff and home based Licence Holders of AES
- All contractors, suppliers and other people working on behalf of AES

It applies to all data that the company 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.
- Data protection risks.

This policy helps to protect AES from some 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 the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities Everyone who works for or with AES 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.

The following roles have key areas of responsibility:

- The AES systems manager is the AES Data Protection Officer and is responsible for:
- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data AES holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's' sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

- The AES marketing and administration manager is responsible for:
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- 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, users of AES systems can request it from the AES systems manager.
- AES will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company 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.

- Employees should request help from the Systems Manager if they are unsure about any aspect of data protection.

Data storage These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Systems Manager. No candidate or customer data should be stored on paper. Paper records on suppliers of AES or employee records should be kept in a secure place where unauthorised people cannot see it.

These guidelines apply to data that is usually stored electronically but have 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.

These guidelines apply to data that is stored electronically:

- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- 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. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- 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 AES 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 and licence holders of AES should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally and only sent by email in the way that a user of AES has been instructed to for business purposes.
- Any data that needs to be sent by email, outside of AES's recruitment activities must be encrypted before being transferred electronically. The AES systems manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers.
- Always access and update the central copy of any data.

Data accuracy The law requires AES 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

AES should put into ensuring its accuracy. It is the responsibility of all users of AES systems who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible with the following guidelines:

- Electronic Data will only be held on Adapt. 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 or email.
- AES will make it easy for data subjects to update the information AES holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer/candidate can't be reached by email or stored telephone number and all reasonable attempts to assess the accuracy of the date have been completed, the data should be removed from the database.
- It is the marketing manager's responsibility to ensure external marketing databases used by AES (outside of Adapt) are checked against industry suppression files every six months.

Subject access requests All individuals who are the subject of personal data held by AES are entitled to:

- Ask what information the company 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 company is meeting its data protection obligations.

If an individual contacts AES requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to colin@aesco.co.uk. The information will then be sent to the individual via a secure method e.g. encrypted email.

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, the Systems Manager will ensure the request is legitimate, seeking assistance from the board of AES or the company's legal advisers where necessary before sharing the data.

Providing information AES 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, the company has a privacy statement, setting out how data relating to individuals is used by the company. [This is available on request. A version of this statement is also available on the company's website.]