General Data Protection Regulations Policy

1.0 PURPOSE:

To give a formal approach that AWS Board of Directors are determined to keep Data protected and not to fall into wrong places causing embarrassment or any type of fraudulent misuse for others to gain from. AWS will use all endeavours to follow the spirit of the General Data Protection Regulations.

2.0 Risk Assessment.

2.1 AWS will risk assess where data is stored and the security arrangements that are in place.

2.2 AWS will ask all third parties that host data information for their policy on data security and what is in place to protect AWS data.

3.0 PROCEDURE:

3.1 **Personnel Data**

3.1.1 All personnel will have to declare personal information upon joining the company or within their time at the company.

3.1.2 All personnel will be given access to a Privacy Notice.

3.1.3 All employees will be informed of their rights under the GDPR 2018 in writing on joining, and retrospectively.

3.1.4 This information will be gathered by Job Application Form, Health Surveillance Form, Health Surveillances, Proof of Identity, Licences, Employment Contracts, Acceptance Letters, Updating personal data information.

3.1.5 Certain information will be held on Next of Kin, Spouse/ Partner's consent to drive a company car. The next of kin, spouse, partner or others will be informed by email of the details held and that all details will be secure, not sold or used for any other purposes. Upon the employees leaving these details will be destroyed.

3.1.6 All personal information will only be seen by relevant persons, Data Process Controller and relevant deputy (ies), employee manager.

3.1.7 Only relevant details of an employee will be passed onto a third party such as training certificates to prove the employee's capability and training to carry out a relevant work task. No personal information will be passed on.

3.1.8 The employee manager will not be allowed to keep any data either by computer or other means, other than for contacting purposes.

3.1.9 All personnel information will be kept in a designated filing cabinet and on a secure data folder. It is the intention over a 12 month period to have all personnel data in secure data folders.

3.1.10 Access to the personnel filing cabinet will be limited to the Data Process Controller and HR manager.

3.1.11 Access to the secure data folder will be limited to the Data Process Controller and HR manager.

3.1.12 As security to our personnel, contractors and members of the public we use CCTV monitoring. No images will be used unless in the case of criminal activity.

3.1.13 At any time, an employee may request to see what Personal Data details are held by AWS. This will be done under the guidance of Data Process Controller and or HR Manager.

3.1.14 Upon leaving the company the employee can request that any Personal Data Details be transferred to their next employment, subject to confidential company information.

Acumen House, Headlands Lane,
Knottingley, West Yorkshire, WF11 0LA

T 01977 529586
W acumenwaste.co.uk

3.1.15 Upon leaving the company the employee can request the company to delete Personal Data Details, subject to information that must be retain for legal purposes as defined by employment legislation.

3.2 **Customer Data Details**

3.2.1 AWS will only keep Business to Business details such as name and address of the company, contact name(s) in the company to conduct business, their business telephone/ mobile numbers, their business emails and the business web details.

3.2.2 AWS will not divulge any company details to any third party unless it is to do with conducting business.

3.2.3 All invoicing details will be kept on a secure server.

3.2.4 All copy paperwork will be kept in a secure room until statutory limitations end, then paperwork will be shredded.

3.2.5 No customer will be contacted by any means unless opted in unless it is to conduct business.

3.2.6 No bank details will be shared with any third parties except for our bank to receive payments.

3.2.7 All contracts of business will not be shared with any third parties unless to execute the business. This will include prices, frequency, type of work.

3.2.8 All customers will be given the opportunity to opt in on receiving marketing information.

3.2.9 All customer data acquired from a third party will only be data that has been approved under GDPR.

3.3 **Supplier Data Details:**

3.3.1 AWS will only keep Business details such as name and address of the company, contact name(s) in the company to conduct business, their business telephone/ mobile numbers, their business emails and the business web details.

3.3.2 AWS will not divulge any company details to any third party unless it is to do with conducting business.

3.3.3 All invoice details will be kept on a secure data base.

3.3.4 All copy paperwork will be kept in a secure room until statutory limitations end, then paperwork will be shredded.

3.3.5 No supplier will be contacted by any means unless opted in, unless it is to conduct business.

3.3.6 No bank details will be shared with any third parties except for our bank to make payments.

3.3.7 All contracts of business will not be shared with any third parties unless to execute the business. This will include prices, frequency, type of work.

3.3.8 All suppliers will be given the opportunity to opt in on receiving marketing information.

3.4 **Web Site:**

3.4.1 The web site will protect the data of employees and permission will be given to use identities such as name and picture.

3.4.2 The web site will not use customer or supplier details without the permission of the customer or supplier.

3.4.3 The web site will refer to GDPR and ask any potential customer or supplier on how they would like to be contacted via an opt in choice.

Acumen House, Headlands Lane,
Knottingley, West Yorkshire, WF11 0LA

T 01977 529586
W acumenwaste.co.uk

3.4.4 No customer or supplier will be sent marketing information unless they opt in.

3.4.5 No data will be shared with third parties, unless that third party is contracted to us and as such that third party will be checked to see if they abide by current data protection legislation.

3.4.6 AWS may use cookies to remember personal settings you have chosen at our website. In no other context do we use cookies to collect information that identifies you personally. Most of the cookies we set are automatically deleted from your computer when you leave our website or shortly afterwards.

3.4.7 Should users wish to deny the use and saving of cookies from this website onto their computer's hard drive, they should take necessary steps within their web browser's security settings to block all cookies from this website and its external serving vendors.

3.5 Emails

3.5.1 AWS will be used for the purpose of business to business use. The sending of emails to private emails in connection of businesses AWS undertake to respect the right and privacy of the private email and will not forward any details to third parties.

3.5.2 AWS emails will make reference to GDPR on the footer of the emails. This will make reference for the recipient, so they can opt in to receive marketing information.

3.5.3 AWS marketing information will be annotated on e-mails as per Appendix 1 to Procedure 12.

3.6 Members of Public

3.6.1 Members of the public will, as a rule not provide Personal Identifiable Information (PII). However, should such information be provided AWS will deal with such provision with positive opt in arrangements as per our consent policy.

3.7 Agency Workers

3.7.1 All agency workers data will be treated in a similar manner as if the agency worker was an employee of AWS.

3.7.2 No agency worker data will be shared with any third party unless in the connection with work.

3.7.3 All data will hold by HR in a secured filing cabinet and secure data server. Only relevant AWS employees will have access to these details for the agency worker to carry out work duties.

3.8 Contract Workers/ Sub Contract Workers

3.8.1 AWS will keep no unnecessary personal data.

3.8.2 AWS reserve the right to know the following information on the worker.

- 3.8.2.1 Name
- 3.8.2.2 Date of Birth to ensure legality to carry out work such as age to drive
- 3.8.2.3 Training records

3.8.3 Any personal information will be kept either in a secure filing cabinet or secure data folder.

3.8.4 Any payments will be made on invoice to the contractor's bank.

3.8.5 Any personal data will be securely destroyed once any statute limitations have passed.

Acumen House, Headlands Lane,
Knottingley, West Yorkshire, WF11 0LA

T 01977 529586
W acumenwaste.co.uk

4.0 Register of breaches

4.1.1 Any breaches of GDPR will be recorded onto the Investigation Log.
4.1.2 The Compliance Manager will investigate the breach.
4.1.3 The Compliance manager will report all findings to the Data Process Controller.
4.1.4 All breaches will be bought to the attention of the Board of Directors.
4.1.5 If a serious breach, then the ICO will be informed.

5.0 Annual Review and Changes

5.1 This procedure will be reviewed once a year unless major changes to the systems take place.
5.2 Any changes in GDPR will prompt this policy and various related Policies and Procedure to be updated.
5.3 Any breaches will initiate a review.

6.0 Security

6.1 Data Process Controller to be briefed and trained on GDPR.
6.2 All authorised data handlers to be brief and trained on GDPR.
6.3 All staff to be trained on GDPR.
6.4 All desks to be clear of all data on leaving the building.
6.5 Only lawful personal information can be sent onto a third party eg training certificates to prove capability to carry out work duties.
6.6 Driving licences not to be sent out to any third parties.
6.7 Any other personal information to have approval of the Data Process Controller or authorised deputy.
6.8 The use of external data storage devices is prohibited unless approval has been given by the Data Process Controller.
6.9 Data will only be kept for the legal minimum time.
6.10 Old data will be destroyed in a proper and legal manner.
6.11 All printing that contains personal data to be recorded by entry into a register kept by the relevant printing machines. The data controller is responsible for checking the record periodically.
6.12 Any lost information is to be investigated by the Data Process Controller or Compliance manager and to follow the non conformance procedure.

Signed and accepted on behalf of the company

Andrew Crossley

Andrew Crossley
Managing Director
1st January 2022

Acumen House, Headlands Lane,
Knottingley, West Yorkshire, WF11 0LA

T 01977 529586
W acumenwaste.co.uk