POL-HR-03 POLICY STATEMENT

Data Protection (GDPR Documentation Toolkit)

1 Overview

1.1 AmcoGiffen takes the security and privacy of your data seriously. The company needs to gather and use information or 'data' about you as part of our business and to manage our relationship with you. The company shall comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. The company has a duty to notify you of the information contained in this policy.

1.2 This policy applies to current, former and perspective colleagues, workers, volunteers, apprentices and consultants. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice the company issue to you from time to time in relation to your data.

1.3 The company has separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subjects. A copy of these can be obtained from the Data Protection Officer.

1.4 The company has measures in place to protect the security of your data in accordance with our Data Security Policies. A copy of this can be obtained from Data Protection Officer.

1.5 The company will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from Data Protection Officer. The company will only hold data for as long as necessary and for the purposes for which the company collected it.

1.6 The company is a '**data controller**' for the purposes of your personal data. This means that the company determines the purpose and means of the processing of your personal data.

1.7 This policy explains how the company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing, or storing personal data in the course of working for, or on behalf of, the company.

1.8 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the company at any time. This policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the company shall comply with the 2018 Act and the GDPR.

2 Data Protection Principles

2.1 Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

The company are accountable for these principles and must be able to show that they are compliant.

3 How the company define personal data

3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of the company or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to the company by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by the company. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

3.4 The company will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender and gender identity;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for the company;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training and development records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video);
- any other category of personal data which the company may notify you of from time to time;
- DBS/Security checks

4 Definition of special categories of personal data

4.1 '**Special categories of personal data**' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

The company will hold and use any of these special categories of your personal data in accordance with the law.

5 Definition of processing

5.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6 How the company will process your personal data?

6.1 The company will process your personal data (including 'special categories' of personal data) in accordance with our obligations under the 2018 Act.

6.2 The company will use your personal data for:

- performing the contract of employment (or services) between the company;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, the company can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that the company stop this processing. See details of your rights in section 12 below.

The company will not use your personal data for an unrelated purpose without telling you about it and the legal basis that the company intend to rely on for processing it.

If you choose not to provide the company with certain personal data, you should be aware that the company may not be able to carry out certain parts of the contract between us. For example, if you do not provide the company with your bank account details the company may not be able to pay you. It might also stop the company from complying with certain legal

obligations and duties which the company have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may have.

7 Examples of when the company might process your personal data

7.1 The company have to process your personal data in various situations during recruitment, employment and even following termination of your employment.

7.2 For example:

- to decide whether to employ you;
- to decide how much to pay you, and the other terms of your contract with the company;
- to check you have the legal right to work for the company;
- to carry out the contract between the company including where relevant, its termination;
- training you and reviewing your performance;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether the company need to make reasonable adjustments to your workplace or role because of your disability;
- to monitor diversity and equal opportunities;
- to monitor and protect the security (including network security) of the company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other colleagues, customers and third parties;
- to pay you and provide pension and other benefits in accordance with the contract between you and the company;
- paying tax and national insurance;
- to provide a factual reference upon request from another employer;
- to pay trade union subscriptions;
- to pay professional bodies;
- monitoring compliance by you, the company and others with our policies and our contractual obligations;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect the company;
- to answer questions from insurers in respect of any insurance policies which relate to you;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure;
- any other reason which the company may notify you of from time to time.

The company will only process special categories of your personal data in certain situations in accordance with the law. For example, the company can do so if we have your explicit consent. If the company asked for your consent to process a special category of personal

data, then the company would explain the reasons for their request. You do not need to consent and can withdraw consent later if you choose by contacting the Data Protection Officer.

7.3 The company does not need your consent to process special categories of your personal data when the company are processing it for the following purposes, which the company may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

7.4 The company may request a DBS check in relation to any criminal convictions, this will be discussed and approved with the colleague before any request is processed, unless it is for a legitimate legal reason such as fulfilling the legal obligation or legitimate interests of the business in relation to it being a condition of a contract.

8 Sharing your personal data

8.1 Sometimes the company might share your personal data with group companies or our contractors and clients/agents/customers to carry out our obligations under our contract with you or for our legitimate interests.

8.2 The company will require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and the company's policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

8.3 The legitimate activities where the company use third parties are:

- Recruitment with the use of agencies
- Occupational health requirements/checks – for medicals, D&A tests, medication reviews etc.
- Private medical provisions
- Pension providers
- Driving licence checks
- Payroll purposes
- Recognition of a trade union and your membership
- Training and compliance – in booking and providing the training required for the role
- To provide benefits such as an EAP and Westfield
- Storing confidential data – HR systems and secure storage

8.4 The company do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

9 How should you process personal data for the company?

9.1 Everyone who works for, or on behalf of, the company is responsible for ensuring data is collected, stored and handled appropriately, in line with this policy and the company's Data Security and Data Retention policies.

9.2 The company's Data Protection Officer is responsible for reviewing this policy and referring any changes for approval to the Board of Directors on the company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to the Data Protection Officer.

9.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

9.4 You should not share personal data informally.

9.5 You should keep personal data secure and not share it with unauthorised people.

9.6 You should regularly review and update any colleague personal data that is processed for legitimate purposes.

9.7 You should not make unnecessary copies of personal data. You should keep or dispose of any copies securely.

9.8 You should use strong passwords to secure any data used. Any documents that are sent via email should be password protected, and the password sent via text message or verbally given to the recipient.

9.9 You should lock your computer screens and any other devices when not at your desk. In order to secure all data, a clear desk policy should be implemented at the end of each day. Consideration should be given when leaving your desk for meetings and breaks.

9.10 Personal data should be encrypted before being transferred electronically to both internal and external contacts. Speak to IT for more information on how to do this.

9.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct may also amount to gross misconduct, under our disciplinary procedure, which could result in your dismissal.

9.12 Do not save personal data to your own personal computers or other devices.

9.13 Personal data should never be transferred outside the European Economic Area except in compliance with the law and with the authorisation of the Data Protection Officer.

9.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

9.15 You should not take personal data away from company premises without authorisation from your line manager or the Data Protection Officer.

9.16 Personal data should be shredded and disposed of securely when you have finished with it. Do not save any data unnecessarily.

9.17 You should ask for help from our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security the company can improve upon.

9.18 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

10 Subject access requests

10.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information the company hold about them. Upon receipt of a SAR you should forward it **immediately** to the Data Protection Officer who will coordinate a response.

10.2 If you would like to make a SAR in relation to your own personal data, the request should be submitted on the Subject Access Request form. The form should then be returned to Data Protection Officer for the company.

10.3 The company will respond within 30 calendar days unless the request is complex or onerous in which case the period in which the company must respond can be extended by a further 2 months.

10.4 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive the company may charge a reasonable administrative fee or refuse to respond to your request.

11 How to deal with data breaches

11.1 The company has a process in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then the company will document and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then the company must also notify the Information Commissioner's Office within 72 hours of discovering the breach.

11.2 If you are aware of a data breach, you must contact the Data Protection Officer immediately and keep any evidence you have in relation to the breach.

11.3 In the event of a data breach against a colleague, the colleague must be informed and notified.

12 Your data subject rights

12.1 You have the right to information about what personal data the company process, how and on what basis as set out in this policy.

12.2 You have the right to access your own personal data by way of a subject access request form (see above).

12.3 You can correct any inaccuracies in your personal data. To do so you should contact the Data Protection Officer.

12.4 You have the right to request that the company erase your personal data where the company are not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the Data Protection Officer.

12.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Data Protection Officer.

12.6 You have the right to object to data processing where the company are relying on a legitimate interest to do so, and you think that your rights and interests outweigh our own and you wish us to stop.

12.7 You have the right to object if the company process your personal data for the purposes of direct marketing.

12.8 You have the right to receive a copy of your personal data and to transfer, or request the company to transfer, your personal data to another data controller. The company will not charge for this and will in most cases aim to do this within one month.

12.9 With some exceptions, you have the right not to be subjected to automated decision-making.

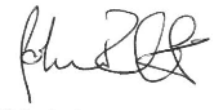
12.10 You have the right to be notified of a data security breach concerning your personal data.

12.11 In most situations the company will not rely on your consent as a lawful ground to process your data. If the company do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Data Protection Officer.

12.12 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

13 Data Protection Officer

13.1 The current Data Protection Officer is **Maria Sykes – HR Director** who can be contacted by email at hr@amcogiffen.co.uk



John Booth
Managing Director