GENERAL DATA PROTECTION REGULATION

GENERAL POLICY

CONTENTS

1. INTRODUCTION

1.1. Avantguard aims to ensure that all personal data and special personal data about employees, clients, suppliers and other appropriate individuals is collected, stored and processed in accordance with the General Data Protection Regulation (2016/679) and the expected provisions of the Data Protection Act 2018 as set out in the Data Protection Bill.

1.2. The General Data Protection (2016/679) Regulation replaces the Data Protection Act of 1998. Its purpose is to protect the 'rights and freedoms' of natural persons and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.3. Information protected under the Regulation includes not only personal data held on electronic devices but also certain manual records containing personal data, for example personnel files that include email addresses and telephone numbers. Personal data such as financial information, which reveals more intimate personal information is considered special personal data and therefore requires a higher degree of consent. The purpose of this policy is to ensure there are no breaches under the General Data Protection Regulation (2016/679).

1.4. This policy meets the requirements of the General Data Protection Regulation (2016/679) and the expected provisions of the Data Protection Act 2018. It is based on guidance published by the Information Commissioners Office on the General Data Protection Regulation and the code of practice for subject access requests.

2. DEFINITIONS

2.1. **PERSONAL DATA:** Any information relating to an identified, or identifiable, individual. This may include (but is not limited to) the individual's name (including initials), identification number, location data and online identifier such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

2.2. **SPECIAL PERSONAL DATA:** Personal data which is more sensitive and therefore requires more protection, this includes (but is not limited to) information about a person's racial or ethnic origin, political opinions, religious or philosophical belief, trade union membership, genetics, biometrics, physical or mental health and sexual orientation.

2.3. **PROCESSING:** Anything done, in an automated or manual process, to personal data, such as (but is not limited to) collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.

2.4. **DATA SUBJECT:** The identified or identifiable individual whose personal data is held or processed.

2.5. **DATA CONTROLLER:** A person or organisation that determines the purposes and the means of processing of personal data.

2.6. **DATA PROCESSOR:** A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

2.7. **PERSONAL DATA BREACH:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3. THE GENERAL DATA PROTECTION REGULATION PRINCIPLES

3.1. There are six General Data Protection Regulation principles that are central to the Regulation. All Avantguard employees must comply with these principles at all times in their information processing practices. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals and must not be processed unless certain conditions are met, in relation to personal and special personal data. These conditions are either that the employee, client, supplier or other necessary individual has given consent to the processing, or the processing is necessary for the various purposes set out in the Regulation. Special personal data may only be processed with the explicit consent of the employee, client, supplier or other necessary individual and consists of information relating to; race or ethnic origin; political opinions and trade union membership; religious or other beliefs; physical or mental health conditions; sexual orientation and criminal offences, both committed and alleged.

- Obtained for only one or more specified, explicit, legitimate and lawful purposes and not further processed in any manner, incompatible with that purpose or those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes shall be in accordance with Article 89(1), which states processing of this nature shall be subject to appropriate safeguards, in accordance with the Regulation, for the rights and freedoms of the data subject. Those measures might include the use of pseudonyms provided that the purpose can be fulfilled in that manner.

- 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 is 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 personal data are processed.

- 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.

4. COLLECTING PERSONAL DATA

4.1. Avantguard will only process data where we have one of six lawful obligations to do so under the Regulation:

- The data needs to be processed so that Avantguard, can fulfil a contract with the individual, or the individual has asked Avantguard to take specific steps before entering into a contract.

- The data needs to be processed so that Avantguard can comply with a legal obligation.

- The data needs to be processed to ensure the vital interests of the individual.

- The data needs to be processed so that Avantguard, can perform the task in the public interest, and carry out its official functions.

- The data needs to be processed for the legitimate interests of Avantguard or a third party (provided that the individual's rights and freedoms are not overridden).

- The individual has freely given clear consent.

4.2. For special categories of personal data, Avantguard will also meet at least one of ten conditions for processing data which are set out in the Regulation:

- Ensure that the individual has given explicit consent to the processing of special personal data for one or more specified purposes.

- Ensure that processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the individual.

- Ensure that processing is necessary to protect the vital interests of the data subject.

- Ensure that processing is carried out in the course of its legitimate purpose with appropriate safeguards, and that the personal data are not disclosed outside the data controller without consent of the data subject.

- Ensure that processing relates to personal data which is manifestly made public by the data subject.

- Ensure that processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

- Ensure that processing is necessary for reasons of substantial public interest.

- Ensure that processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems.

- Ensure that processing is necessary for reasons of public interest in the area of public health.

- Ensure that processing is necessary for archiving purposes in the public interest.

5. THE DATA CONTROLLER

5.1. Avantguard processes personal data relating to employees, customers, suppliers and other necessary individuals, and therefore is a data controller. Avantguard Security Limited (Company number: 6789692) is registered as a data controller with the Information Commissioners Office and will renew this registration annually or as otherwise legally required.

5.2. **DATA PROTECTION OFFICER:** The data protection officer is responsible for overseeing the implementation of this policy, monitoring our compliance with the Regulation, and developing related policies and guidelines where applicable. The data protection officer is also the first point of contact for individuals whose data Avantguard processes, and for the Information Commissioners Office. Full details of the data protection officer's responsibilities are set out in their job description.

- Our data protection officer is Anthony Woolcott and is contactable at aww@avantguardsecurity.co.uk

6. **LIMITATION, MINIMISATION AND ACCURACY**

6.1. Avantguard will only collect personal and special personal data for specified, explicit and legitimate reasons. We will explains these reasons to the individual when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individual concerned before we do so, and seek consent where necessary. When Avantguard no longer needs personal data they hold, we will ensure it is deleted or anonymised.

7. THIRD PARTY DATA PROCESSING

7.1. Avantguard will only work with third party processors who policies and statements are in line with General Data Protection Regulation.

7.2. Avantguard will carry out assessments and audits where necessary, to ensure third party processors are aware and working in line with the General Data Protection Regulation.

7.3. For more information about our third party processors and the data we share with them can be provided through our data protection officer.

8. DIRECT MARKETING AND DATA PROCESSING

8.1. Avantguard only collects personal data which does not include any special personal data, for example, name address and email. Avantguard will obtain explicit consent from the individual to hold this data.

8.2. Avantguard are required to collect personal data about clients and potential clients in order to provide them with important information about services in line with contracts or business we provide, or extra services you might be of interest. Avantguard will not collect personal data from individuals that we do not need in order to provide and oversee contracts or services.

8.3. All personal data in relation to direct marketing that Avantguard processes is only accessed by authorised employees.

8.4. Personal data that Avantguard holds for marketing purposes is kept until an individual(s) notifies Avantguard that they no longer wish to receive marketing information. At this point, all personal data and email correspondence will be removed.

9. INDIVIDUALS RIGHTS TO ACCESSING PERSONAL DATA IN REGARDS TO MARKETING

9.1. Under the Regulation, individuals have the right on request to receive a copy of the personal data that Avantguard holds about them, including personal data held on Avantguard's customer relationship management system, and to demand that any inaccurate data that is held, should be corrected or removed. They also have the right to lodge a complaint with a supervisory authority, to seek compensation where damage and distress has been caused to them as a result of any breach of the Regulation by Avantguard.

9.2. Individuals are entitled to request the following information under the Regulation:

- The purpose of the personal data being processed;
- The categories of personal data concerned;
- The recipients to whom personal data has been or will be disclosed to;
- The envisaged period for which the personal data will be stored, or, if that is not possible, the criteria used to determine that period;
- Any available information as to the source of data information will be given, where the personal data is not collected by Avantguard,
- To be informed in certain circumstances of the logic involved in computerised decision making.

9.3. Upon request, Avantguard will provide individuals with a statement regarding the personal data held about them. This will state all the types of personal data Avantguard holds and processes about the individual and the reasons for which they are processed.

9.4. If individuals wish to access a copy of any personal data being held about them, they must fill out a Subject Access Request Form which you can request by emailing the data protection officer (Anthony Woolcott – aww@avantguardsecurity.co.uk). This information will be provided free of charge. However, Avantguard reserves the right to charge £10.00 for requests that are manifestly unfounded or excessive, in particular repetitive requests. Requests for further copies of information already provided will be charged at £10.00.

9.5. Avantguard will respond promptly to subject access requests within 30 calendar days of receiving the request. When responding to requests Avantguard may:

- Ask the individual to provide two forms of identification.
- Contact the individual via telephone to confirm the request was made.

9.6. Avantguard may extend the response time by a further 30 days where requests are complex or numerous. In this case, Avantguard will contact the individual within 30 days of the receipt of the request and explain why the extension is necessary.

9.7. Avantguard reserves the right to refuse to respond to a request, where a request might be deemed manifestly unfounded or excessive, in particular because they are repetitive. Where this is the case, Avantguard will explain to the individual why the request has been refused. At this point, the individual has the right to complain to the Information Commissioners Office and to a judicial remedy without delay. If the individual wishes to make a complaint, this must be submitted to the Information Commissioners Office within 30 days of the written communication from Avantguard.

10. PHOTOGRAPHS AND VIDEOS

10.1. As part of the social media and marketing process, Avantguard may take or acquire photographs. Avantguard will obtain consent for these photographs to be used on our social media or marketing materials.

10.2. Consent can be withdrawn at any time during employment and this will not affect your employment contract. If consent is withdrawn, any photographs with that individual will be deleted and will not be used in further promotional material. However, if the image(s) have been used on past social media posts or marketing materials, it may be beyond Avantguard's control to completely remove the image(s).

10.3. CCTV is used in the Avantguard Head Office to ensure it remains safe. Avantguard will adhere to the Information Commissioners Office code of practice for the use of CCTV. Avantguard does not need to ask individual(s) permission to use CCTV, but we will make it clear where individuals are being recorded. Security Cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

10.4. Any enquiries about the CCTV system should be directed to Anthony Woolcott: aww@avantguardsecurity.co.uk

11. DATA SHARING OUTSIDE OF THE EUROPEAN ECONOMIC AREA

11.1. If Avantguard is required to share data, we will ensure that the third party is compliant with the General Data Protection Regulation.

12. **DATA PROTECTION BY DESIGN AND DEFAULT**

12.1. Avantguard will put measures into place to show that we have integrated the general data protection regulation into all of our data processing activities including:

- Appointing a suitably qualified data protection officer, and ensuring they have the necessary resources to fulfil their duties and maintain expert and up to data knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in section 3.
- Completing privacy impact assessments where Avantguard's processing of personal data presents a high risk to the rights and freedoms of individuals, and when introducing new technologies.
- Integrating data protection into internal documents including this policy, and related policies and privacy notices.
- Training employees on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we continue to be compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our data protection officer and all information we are required to share about how we use and process personal data.
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

13. DATA SECURITY AND STORAGE OF RECORDS

13.1. Avantguard will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

13.2. In particular, paper based records will be kept in a code locked cupboard and only authorised employees will have access to this. The code will be changed when authorised employees change.

13.3. Portable electronic devices, such as mobile phones, tablets and handhelds that contain personal data will be kept in a locked cupboard when not in use.

13.4. Passwords are at least 8 characters long that are used to access work computers, where employees are reminded to change this password every 12 months.

13.5. All portable devices and removable media such as tablets and handheld devices run the latest Android operating system and are therefore encrypted.

13.6. Employees are not allowed to store client personal on their personal devices data during or after the course of their employment with Avantguard.

14. PERSONAL DATA BREACHES

14.1. Avantguard will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, Avantguard will follow the procedure set out in section 16. Where appropriate, Avantguard will report the data breach to the Information Commissioners Office within 72 hours.

15. DATA BREACH PROCEDURE

15.1. This procedure is based on the guidance on personal data beaches produced by the Information Commissioners Office. On finding or causing a breach, or potential breach, the employee or data processor must notify the data protection officer immediately.

15.2. The data protection officer will investigate the report and determine whether or not a breach has occurred. To decide, the data protection officer will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

15.3. The data protection officer will alert the managing director and will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant employees or data processors where necessary. The data protection officer will assess the potential consequences, based on how serious they are, and how likely they are to happen.

15.4. The data protection officer will work out whether the breach must be reported to the Information Commissioners Office. This must be judged on a case-by-case basis. To decide, the data protection officer will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage, including through:

- Loss of control of their data
- Discrimination
- Identify theft of fraud
- Financial loss
- Unauthorised reversal if psuedonymisation
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned.

15.5. If it is likely that there will be a risk to people's rights and freedoms, the data protection officer must notify the Information Commissioners Office within 72 hours. The data protection officer will document the decision (either way), in case it is challenged at a later date by the Information Commissioners Office or an individual affected by the breach.

15.6. In cases where the Information Commissioners Office must be notified, the data protection officer will do this by visiting the 'report a breach' page on the Information Commissioners Office website. As required the data protection officer will set out:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned.
- The name and contact details of the data protection officer.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

15.7. If all of the above details are not yet known, the data protection officer will reports as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the data protection officer expects to have further information. The data protection officer will submit the remaining information as soon as possible.

15.8. The data protection officer will also assess the risk to individuals, again based on the severity and likelihood of potential and actual impact. If the risk is high, the data protection officer will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the data protection officer.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

15.9. The data protection officer will also:

- Notify any relevant third parties who can help mitigate the loss to individuals.
- The data protection officer will document each breach, irrespective of whether it is reported to the Information Commissioners Office. For each breach the record will include: facts and cause, effects and action taken to contain and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).
- Ensure that records of all breaches are stored appropriately.
- Will meet with the management to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

16. ACTIONS TO MINIMISE THE IMPACT OF DATA BREACHES

16.1. Avantguard will take actions to mitigate the impact of different types of data breach, focussing especially on breaches involving particularly risky or sensitive information. Avantguard will review the effectiveness of these actions and amend them as necessary after any data breach. For example, password protecting any sensitive information that is sent via email.

16.2. Information about Avantguard's IT Infrastructure is available from the Avantguard Data Protection Officer.

17. TRAINING

17.1. All employees are provided with data protection training as part of their induction process.

17.2. Any changes to the General Data Protection Regulation will be provided to all employees either by written communication or training.

18. MONITORING ARRANGMENTS

18.1. The data protection officer is responsible for monitoring and reviewing this policy.

18.2. This policy will be reviewed and updated where necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect Avantguard's practice. Otherwise, or from then on, this policy will be reviewed every one year and shared as required.

19. LINKS WITH OTHER POLICIES

19.1. General Data Protection Employee Policy (SF PD 006b)

19.2. General Data Protection Client Policy (SF PD 006c)

19.3. General Data Protection Regulation Privacy Statement