PRIVACY POLICY

Introduction & Overview

Secure Facilities Management Limited (Secure) is committed to ensuring that Data Privacy and article 9(2)(a) where you have Data Security are the top priority. Secure is compliant with the Data Protection Act (1998) and with the General Data Protection Regulation (GDPR) from May 2018.

Definitions

Secure uses 'personal data', including that relating to clients, candidates, staff, third parties and business contacts, in the course of day to day business. In doing so, we must act in accordance with the Data Protection Act 1998 (DPA). The DPA establishes a framework of obligations to protect personal data and the rights of 'data subjects'

The DPA applies to all personal data which is 'processed'. 'Processed' data includes data which is collected, stored, altered, organised, disclosed, destroyed etc.

'Data' means information which –

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (c).

'"**Personal data**" – any information relating to an identified or identifiable natural (living) person ("**data subject**") from which that person can be identified directly or indirectly from an identifier such as name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Sensitive personal data**" – personal data revealing racial or ethnic origin, political opinion, religious or philosophical belief, trade union membership, the processing of genetic or biometric data for the purposes of identifying a data subject, data concerning health or data concerning a person's sex life or sexual orientation.

"**Data Controller**" – means a natural or legal person, public authority, agency or other body which alone, or jointly with others, determines the purposes and means of the processing of personal data.

"**Data Processor**" – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"**Data Subject**" – an identified or identifiable natural person. This includes any individual we process data in respect of the DPA

Regulatory References

Data Protection Act (1998):

- Regulates the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. DPA will be replaced by the GDPR (General Data Protection Regulation) in May 2018.

Data Loss Prevention (DLP):

- Refers to the act of prevent the loss of data, in particular sensitive client data and confidential company information. DLP typically focusses on securing email, mobile devices, USB storage devices and network access.

Scope

This policy is mandatory and applies to all Secure employees and all departments. This Policy sets out the procedures which must be followed to enable Secure to comply with legal obligations as well as obligations to its clients under current contracts.

Secure's Management must ensure that all employees are aware of this policy and procedures. It is the responsibility of all employees to comply with this policy.

Any non-compliance with this policy must be logged with David Fitzjohn Exceptions to this policy must be approved by the Line Manager and if warranted by a Director.

Failure by any employee of Secure to comply with the procedures set out in this Policy may lead to disciplinary action being taken against them; up to and including dismissal.

Periodic internal audits or reviews will be conducted in order to verify that the policy is appropriately implemented.

Policy Requirements

You must:

- Process data fairly and in an authorised manner, which means only in respect of the legitimate purposes that the data was obtained and only in accordance with the expectations of the data subject.
- Ensure that any personal data held is adequate, relevant and not excessive.
- Ensure that any personal data held is accurate and where necessary, up to date.
- Remember that the information held on our files and systems (including emails) may be disclosed to the data subject. Any comments made about an individual must therefore be professional and objective.
- Ensure that personal data is held for no longer than is necessary. This will vary depending on the type of information.
- Ensure that adequate data security safeguards are in place, both within the office and when working away from the office, to make sure that information is not lost, stolen or otherwise disclosed to unauthorised persons.
- Ensure that all documentation or other materials that are no longer required and which contain personal data are disposed of securely.
- Ensure that contracts with service providers, consultants or other third parties providing services for the firm have the appropriate terms in place to control the use of the data and to maintain adequate levels of data security.
- Undertake the firm's compulsory training on Data Protection and information security.

You must not:

- Disclose personal data to anyone other than the data subject unless you have their consent, or it is under one of the exemptions to the DPA. If you are uncertain do not disclose anything until you have clarified the position.

You can be prosecuted individually if you deliberately misuse or deliberately disclose information that you are not authorised to use or disclose.

There are detailed rules that apply to the disclosure of data and international transfers. Advice should be sought from David Fitzjohn in such cases.

Security Checks

Inbound Calls – On all inbound calls, prior to disclosing any information the following (where available) must always be confirmed correctly by the client –

- Clients or Candidates full name
- First line of address
- Postcode
- The Candidate's full date of birth

Outbound Calls – On all outbound calls, prior to disclosing any information the following (where available) must always be confirmed correctly by the client –

- Client confirms you are speaking to the correct person achieved by asking to speak to client using their full name
- First line of address
- Postcode
- The Client's full date of birth

3rd Party Calls – Where a third party authority is held, the following security questions must always be asked and answered correctly before being able to discuss an account with the authorised representative –

- Clients full name
- First line of address
- Postcode
- The Client's full date of birth
- Password (if this has been provided)

In person – Prior to discussing accounts in person with a client, proof of identity should be requested, such as passport, driving licence. Where this is not available non photographic ID such as debit/credit card, recent bill may be used in conjunction with verification of the client's full date of birth.

Via e-mail – Prior to responding to e-mails received from clients, we must first satisfy that the e-mail account is that of the client. In order to do this we must request that the client answers the standard

DPA questions via e-mail before responding to the original query. Once DPA questions have been satisfied the client's e-mail should be updated within the system to display verified. Once verified we may respond to further e-mails without the need to complete e-mail DPA verification again. The e-mails documenting e-mail DPA verification must be scanned to the case. Alternatively e-mail addresses can be verified over the phone once verbal DPA has been completed.

Where standard DPA questions are not possible due to a lack of verification data, we should use other account data in order to formulate specific questions that will enable us to identify that we are dealing with the correct person. Examples could be verifying the last payment amount/date on the account, product type, etc.

3rd Party Authorities

When requested to do so by a client, we will deal with a nominated third party on behalf of the client. Before we can deal with a 3rd party we must obtain a valid authority. This can be received either written or verbally from the client.

Verbal Authority – After a client themselves have passed through security successfully they may nominate another person to take over the call, or call in later that day to act on behalf of themselves. The client should provide the full name of the person they wish to authorise and their relationship to the nominated party.

It is important to note that when a client gives us a verbal authority, this will last only until close of business on the day it is received. Should the client require us to continue to deal with the same nominated third party then we will require verbal authority to be provided again, or for a longer term solution the client may wish to provide a written authority.

Written Authority – Client's that require a longer term authority in place or who wish to permanently give an authority to another person to deal with an account must write to us and provide this information in a written format via a letter of authority. They must provide the full name of the person they wish to authorise and the relationship of the authorised person to the client along with an indication of how long the authority will last for. Where it has not been stipulated that an authority is for a specific time then the authority will be deemed to be on-going. The letter of authority must be signed and dated by the client before we can accept the instruction from the client.

Subject Access Requests

All staff receiving a subject access request must notify David Fitzjohn immediately.

Any written request for personal data or other requests referring to an individual's private data should be treated as a subject access request. There does not need to be any reference to the DPA for the request to be valid. A written request can include an email.

Requests must be dealt with within 40 calendar days of a valid request being received (a request together with the required fee and any necessary proof of identity).

Information Security

Information within the business must be kept secure. The Information Commissioner has the authority to fine organisations where personal data is lost, misdirected or misused. The fines can be substantial. There is also the risk of complaints, negligence claims or of adverse publicity.

Care should be taken to ensure that contact details are correct when any information is sent or transmitted. A greater level of care is required when dealing with sensitive personal data, which includes information about a person's racial or ethnic origin, medical information, religious or political beliefs, trade union membership, sexual life or the commission of any criminal offence.

Where sensitive personal data is offered by a client, authority should be sought from the data subject prior to recording the data along with an explanation of why we would like to record the information. Typically, this will be in order that we can better manage a client's account taking into account any such extenuating circumstances or vulnerability.

No information should be taken out of the office on an electronic device unless sufficient technical safeguards are in place, in accordance with current IT policy.

Data Security Breaches

A Data Security breach could occur where client data has been processed without appropriate measures being taken to protect the data. Examples of a Data Security breach could be:

- Personal information being shared with a Client without having first completed identification checks
- Client information being sent electronically to a 3rd party without appropriate authorisation, encryption or password protection
- Non-adherence to Secure's 'Secure Desk' policy; for example, Client information being written down and left unattended at any time

A Data Protection breach could occur where data is obtained or viewed by a person that was not authorised to receive it. Some examples of a Data Protection breach could be:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment Failure

- Hacking
- Social Engineering offences where information is obtained by a third party by means of deception

David Fitzjohn will maintain a log of data breaches and provide any necessary support in managing and resolving the breach.

Managing a Data Breach

- Following notification of a data breach Secure will establish a recovery plan to minimise any risk of damage to the individuals affected and to the business.
- Consider the potential adverse consequences of the breach and take steps to minimise or remove such risks.
- Recover any documents or data promptly. You should not agree to the recipient destroying documents themselves.
- Consider who you should to notify to contain or minimise any impact on the individuals affected, our clients and the business.
- Act quickly to investigate the breach and consider improvements to systems to prevent future breaches.

Reporting

A differentiation is made between a security incident (ex. Malware infection or Crypto Locker outbreak) vs Data Breach (loss of personal information). In the case of the latter, the ICO would be informed as per requirements in the Data Protection Act and GDPR from May 2018. The ICO must be informed of a Data Breach within 72 hours.

See Appendix B for further details.

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/

Client communication regarding lesser security incidents would be assessed on a case by case basis and in line with agreed client SLA's.

To Report a Data Breach

Call the Information Commissioners Office:

0303 123 1113 option 3

Complete the Breach Reporting form in Appendix C

Version History

Policies are reviewed annually as a minimum. Amendments to policies are reviewed and approved by the Board.

Author/Reviewer	Description of Change	Date of Revision	Version
David Fitzjohn	Policy written	17/05/2018	V1.0

The following statement explains Secure's policy regarding the personal data you may disclose to us when you wish us to process personal information to enable us to provide advice and professional services as an employment agency, to assist you with seeking work, to maintain our own accounts and records and to support and manage our employees

Our aim is to respect your privacy and comply with the Data Protection Act 1998 and the General Data Protection Regulation (GDPR).

The Data Controller

Secure Facilities Management Limited is the Data Controller for any personal data you give to us. Our full details are:

4 Summerhouse Rd
Northampton
NN3 6BJ

Telephone: 0333 241 4180
Email: info@securefacilities.com

What Personal Data We Collect and What We Do With It and our Legal Basis for Doing so

We will only collect personal information from you necessary for us to carry out our functions and activities. We may collect personal information from you in person, over the telephone, via application forms, via email, upon your visit to our website, or from a third party.

We will only collect special category information (sensitive) from you where processing is necessary for the purposes of carrying out our obligations and exercising our specific rights, or your rights in

the field of employment providing for appropriate safeguards to your fundamental rights and interests, or with your explicit consent. Sensitive information means information relating to your race; ethnic origin; political opinion; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

In general, the special category information we collect and hold will be limited and relevant to your ability to fulfil a potential employment opportunity, or to make a reasonable adjustment. If this includes information about your physical or mental health, such information will only be used by us to assess your requirements for reasonable adjustments. We will not share or disclose it to others.

If you have provided consent, you can withdraw your consent as anytime by contacting us. Please note that we may not be able to process your request for Reasonable Adjustments if you do this.

If we collect your personal information (and this can include special category data) from a third party we will take reasonable steps to make you aware of this and which third party has provided the data. When collecting personal information, we will use lawful and fair means.

How Long We Keep Your Personal Data

We will retain basic information about you for a minimum of 7 years for tax purposes, for the establishment, exercise or defence of legal claims and for commercial purposes. Subject to any legal requirement, we will delete your information where you tell us that you will no longer wish to be registered with our organisation, or 7 years after our last engagement with you.

Third Parties

We will disclose your personal information on a confidential basis to our clients where you have applied for a position in connection with a vacancy we are facilitating for that client.

We may also disclose your data to external service providers so that they can provide services such as financial or administrative services in connection with the operation of our business; and to any person (where necessary) in connection with their services, such as law enforcement, regulatory authorities or advisors.

If we engage external service providers, we will take reasonable steps to ensure those entities comply with their obligations under the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) when they handle your personal information. We will also ensure external service providers are only authorised to use personal information for the limited purposes specified in our agreement with them

Protecting Your Personal Data

We are committed to ensuring that your personal data is secure. In order to prevent unauthorised access or disclosure, we have put in place appropriate technical, physical and managerial procedures to safeguard and secure the information we collect from you.

Cookies

Many websites place cookies whenever a user visits their site, in order to track traffic flows. Cookies are text files, which identify your computer to the server. Secure Payroll may use cookies from time to time. Please see our Cookie Policy.

Links to Other Sites

Our web site contains links to other web sites. We are not responsible for the privacy practices of such other sites. When you leave our site please be sure to read the privacy statements of each and every web site that collects personal data about you. This privacy policy applies solely to information collected by Secure Payroll Ltd.

Your Rights

You are in complete control. You can object or withdraw your consent to the use of your personal data at anytime, although in some cases we may not be able to provide your requested service where the information processing is an integral part of the service or where we have a legal obligation to process your information. We will tell you if this is likely to be the case.

Subject to some legal exceptions, you have the right to:

- request a copy of the personal information Secure Payroll holds about you;
- to have any inaccuracies corrected;
- to have your personal data erased;
- to place a restriction on our processing of your data;
- to object to processing; and
- to request your data to be ported (data portability).

To learn more about these rights please see the ICO website.

Please address any such requests to the Secure Data Protection Officer through the contacts page.

If you are dissatisfied with our response you can complain to the Information Commissioner's Office

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113 (local rate) or 01625 545 745
Fax: 01625 524 510

Your Data Abroad

We do not transfer or process data outside the European Economic Area unless we have your specific consent, or where the nature of the processing requires it (for example, because you have chosen to use an email or other communications service which routes data outside the EEA) or where a client's HR or Payroll Department may be located outside the EEA. Where we do require to transfer personal information we shall ensure that the organisation receiving the personal data has provided adequate safeguards, that you rights can be enforced and effective legal remedies exist following the transfer.

Adequate safeguards may be provided for by a legally binding agreement between public authorities or bodies; binding corporate rules (agreements governing transfers made between organisations within in a corporate group); standard data protection clauses in the form of template transfer clauses adopted by the Commission; standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission; compliance with an approved code of conduct approved by a supervisory authority; certification under an approved certification mechanism as provided for in the GDPR; contractual clauses agreed authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority

Last update: May 2018