ISO 9001 EN 1090
ISO 14001 ISO 3834-2
OHSAS 18001 VCA
EFQM

EIFFAGE SMULDERS

P-HRM-SPU-003

Data Protection Policy

Rev.	Date	Description	Author	Validated by	Approval date IMS
2-1	30/05/2019	Amendments to 2019 Revision	Amanda Young	Tom Coosemans	
2-0	25/03/2019	2019 Revision	Amanda Young	Tom Coosemans	
1-1	01/10/2018		Tina McKeown/Graham Brooks	Tom Coosemans	
1-0	25/05/2018	First issue	Heather Kipling	Tom Coosemans	31/05/2018

Contents

1 Introduction

In order to operate efficiently, Smulders needs to collect and use information about the people that we work with. The correct and lawful treatment of personal information is integral to a successful operation and is also important in maintaining the confidence of the people we work with. Smulders fully endorses and agrees to adhere to the principles of the General Data Protection Regulation (EU) 2016/679 (**GDPR**) and the Data Protection Act 2018 (together the **Data Protection Legislation**).

2 Scope

This policy covers the Smulders Projects Limited UK Newcastle (Wallsend) facility, hereinafter referred to as the Company and applies to all personnel, to include employees, agency workers, contractors and sub-contractors. It is the responsibility of personnel to ensure this policy is adhered to if applicable by any visitors that may come into contact with personal information; depending on the nature of the visit.

3 Personal Data

Personal data is any data relating to a living individual (a **data subject**) who can be identified from that data (or from that data combined with other information in our possession), in particular by reference to an identifier such as a name or an ID number or a location, job title etc. Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

When processing this information, it must be in line with the principles set out in section 4 of this policy.

All personal data should be treated with the utmost confidentiality and only shared with those who need it and access it through appropriate channels. It should never be disclosed to un-authorised personnel either within the company or externally. The Company's Privacy Notice sets out further information on this matter and can be found on SharePoint.

4 Data Protection Principles

Personal information must be:

1. processed fairly and lawfully and in a transparent manner;
2. processed only for the purposes for which it was not collected;
3. adequate, relevant and limited to what is necessary;
4. accurate and up to date;
5. kept in a form which identifies data subjects for no longer than is necessary for the purposes data is processed; and
6. processed in a manner that ensures appropriate security of the personal data.

5 Lawful Bases

The Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. These are:

1. the data subject has consented to the processing;
2. processing is necessary for the performance of a contract;
3. processing is necessary for compliance with a legal obligation;
4. to protect vital interests of the data subject or another person;
5. for the performance of a task carried out in the public interest; or
6. for the purpose of the legitimate interests pursued by the controller or by a third party.

The Company has established its lawful bases for processing, and will not process personal data for any further purposes without first establishing there is a lawful basis for doing so.

6 Your Personal Data

All data subjects, whether personnel, contractors, visitors customers or clients, will be informed if the Company processes their personal data. The privacy notice for how we process staff and personal data is Newcastle privacy notice and is available from the HR Manager or Security.

7 Sensitive Personal Information

There are special categories of personal data, which include information about a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Special category personal data can only be processed if there is an additional lawful basis for doing so, such as for health care purposes, or to comply with employment or social security law. The Company has established its lawful bases for processing special category personal data, and will not process personal data for any further purposes without first establishing there is a lawful basis for doing so.

Special category personal data should be processed using organisational and technical security measures appropriate to the sensitivity of that data.

8 CCTV

The Company operate a closed circuit television (CCTV) system, at the Newcastle (Wallsend) facility which records images to protect the Company's property and to provide a safe and secure environment for staff, temporary workers, sub-contractors and for visitors to the Company's business premises such as clients, customers and suppliers. The **CCTV Policy P-HRM-SPU-001** sets out the use and management of the CCTV equipment and images in compliance with Regulation (EU) 2016/679 the General Data Protection Regulation and the Data Protection Act 2018 (Data Protection Legislation). Further information relating to the management of your personal information, including the use of CCTV is contained within the **Smulders Newcastle Privacy Notice D-HRM-SPU-003**.

9 Data Storage

The Data Protection Legislation requires the Company to implement appropriate technical and organisational measure to keep personal data secure, including to store data. A lot of it is just common sense.

Hard copies of personal information should be stored as follows.

- Kept in a secure place where unauthorised people cannot see it, for example a fireproof filing cabinet.
- Ensure no copies are left at photocopiers/printers.
- Ensure personal information is shredded and disposed of securely when no longer needed.

Electronic data should:

- be protected from unauthorised access, accidental deletion and malicious hacking attempts;
- be protected by strong passwords that are changed regularly and never shared between personnel;
- be locked away securely if stored on removable media (when not in use) and all such devices should be encrypted; and
- only be stored on designated drives and servers allocated by ICT; and
- never be saved to laptops/tablets/mobile phones.

Folders containing personal data should only be shared with those that need access, and ICT ensure that personal data is sited in a secure location, backed up frequently and protected by security software and a firewall.

10 Data Use

Personal data must be accurate and relevant for the purposes in order for the Company to make use of it and to comply with the Data Protection Legislation. However, when it is accessed and used it is at the greatest risk of loss, corruption and theft. To help safeguard the data the Company holds and processes, it is important that the following is observed:

- Ensure that computer screens are always locked when left unattended.
- Personal data must not be shared informally.
- Advice should be sought from the Company Director to ensure we have a lawful basis to share data with external contacts.
- Advice should be sought from ICT on how best to transfer data electronically to authorised external contacts.
- Personal and company data must not be saved to personal devices.
- Personal data should not be transferred outside of the European Economic Area unless there is an appropriate safeguard in place to legitimise the transfer.
- Duplicated personal data must be held in as few places as necessary.
- Personnel should take every opportunity to ensure that data is updated when changes occur and inaccuracies are discovered.

11 Access

Data subjects have the right to access their personal data held by the Company, under the Data Protection Legislation. Data subjects have the right to confirmation as to whether their data is being processed and for what purpose. Any individual wishing to access their personal data should complete a Subject Access Request Form **D-HRM-SPU-004** . The form is available via your recruitment agency, internally via the HR department or on the Company Sharepoint system, once completed it should be sent to the HR Manager at the Newcastle (Wallsend) facility.

It is important that a data subject provides the required information for the Company to action the Subject Access Request. The Company must respond within 30 calendar days of receiving sufficient information to action the request. The Company will ask you to verify your identity before releasing any information to you. The data will be released in an electronic format as outlined by the GDPR unless another format has been requested.

12 Data Subject Rights

The Company will process all personal data in line with data subjects' rights, in particular the right to:

1. be informed on what personal data is being processed (see section 6 of this policy);
2. request access to any data held about them by a data controller (see section 11 of this policy);
3. object to processing of their data for direct-marketing purposes (including profiling);
4. ask to have inaccurate or incomplete data rectified;
5. be forgotten (deletion or removal of personal data);
6. restrict processing;
7. data portability;
8. not be subject to a decision which is based on automated processing; and
9. complain to the data protection regulator, the Information Commissioner's Office.

Employees should be aware that not all data subjects' rights are absolute, and any requests regarding the above should be immediately reported to the Information Security Officer.

13 Exemptions

Personal data processed for some specified purposes is exempt from some of the provisions of the Data Protection Legislation, such as data subject access and erasure requests.

This also allows companies to disclose information to law enforcement agencies without the consent of the data subject. Under such circumstances, the Company is able to disclose personal data however will first ensure that the request is legitimate and seek advice from the Company's legal advisors where necessary.

14 Retention and Disposal

Under the Data Protection Legislation, data should not be kept for any longer than is necessary for its intended purpose. In order to satisfy this requirement, the Company will conform to UK retention period guidelines. The Company's **Retention Policy P-HRM-SPU-002** provides further details.

All hard copies of personal data will be shredded before disposing of and electronic data will be deleted in line with ICT governance procedures.

15 Data Breaches

Personal data must be managed in accordance with the Data Protection Legislation. In the unlikely event of there being a data breach, the appropriate action must be taken. Personal data breaches can include:

- Access by an unauthorised third party.
- Deliberate or accidental action by a controller or a processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data.

In line with GDPR, in the unlikely circumstances where a data breach is likely to result in a risk to the rights and freedom of an individual, the Company must notify the individuals concerned as soon as the breach has been identified and put measures in place to prevent a further breach.

The Company must notify Smulders Belgium when they first become aware of the breach as they have a duty to notify the Information Commissioners Office (ICO) within 72 hours of becoming aware of the breach.

16 Concerns

Any concerns or complaints about the handling/storage of the data should be raised with the HR Manager on +44 (0)191 2956728.

17 Other Documents

Other documents to be read in conjunction:

P-HSM-SPU-001	Yard Agreement
P-HSM-SPU-011	Code of Conduct
D-HRM-SPU-003	Smulders Newcastle Privacy Notice
P-HRM-SPU-002	Retention Policy