Data Protection Policy

1 Introduction and Scope

1.1 This policy sets out how H&M Security Services Ltd handle the personal data of customers, suppliers, partners, employees, workers, and other third parties.

1.2 This policy is about your obligations under the data protection legislation. Data protection is about regulating the way that the Company uses and stores information about identifiable people (Personal Data). It also gives people various rights regarding their data - such as the right to access the Personal Data that the Company holds on to them. We try to avoid using legalese or jargon in this Policy; however, certain words and phrases have particular meanings under data protection legislation.

1.3 During the course of our business, we will collect, store and process Personal Data about our Staff, customers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in the Company and will ensure that the Company operates successfully.

1.4 This policy is aimed at all Staff working in the Company (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities ('you').

1.5 You are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

1.6 This policy does not form part of your contract of employment and may be amended by the Company at any time.

1.7 The Data Protection Officer (DPO) / Information Manager is responsible for helping you to comply with the Company's obligations. All enquiries concerning data protection matters should be raised with Brian Tuite or his authorised deputy.

2 What information falls within the scope of this policy

2.1 Personal Data at work: In order for you to do your job, you will need to collect, use and create Personal Data. Virtually anything that relates to a living person will include Personal Data.

Examples of places where Personal Data might be found are:

2.1.1 on a computer database based at one of the Companies locations.
2.1.2 in a file, such as a personnel or client record.
2.1.3 in a register or contract of employment.
2.1.4 letters, attendance notes, meeting minutes and other documents or written records.
2.1.5 Medical. records

2.1.6 email correspondence.

2.2 Categories of Critical Company Personal Data

The following categories are referred to as Critical Company Personal Data in this policy. You must be particularly careful when dealing with Critical Company Personal Data which falls into any of the categories below:

2.2.1 physical or mental health or condition.
2.2.2 racial or ethnic origin.
2.2.3 religious beliefs or other beliefs of a similar nature
2.2.4 trade union membership.
2.2.5 information relating to actual or alleged criminal activity.
2.2.6 genetic or biometric information.

If you have any questions about your processing of these categories of Critical Company Personal Data, please speak to the DPO.

3 The Principles of Data Protection

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

3.1 Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

3.2 Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
- Accurate and where necessary kept up to date (Accuracy).
- Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
- Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4 Personal Data must be processed fairly, lawfully and transparently

4.1 "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.

4.2 People must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office ("ICO") (the data protection regulator).

4.3 This information is often provided in a document known as a Transparency Notice. Copies of the Companies' Transparency Notices can be obtained from the DPO. You must familiarise yourself with the Company's Staff, Customers and other suppliers.

4.4 Transparency Notices.

4.4.1 You must only process Personal Data for the following purposes:

(a) as set out in the applicable Transparency Notice.

(b) protecting and promoting the Company's legitimate interests and objectives (for example to promoting the business.

(c) to fulfil the Company's contractual and other legal obligations.

4.5 Use of Personal Data: If you want to do something with Personal Data that is not on the above list, you must speak to the DPO. This is to make sure that the Company has a lawful reason for using the Personal Data.

4.6 If you are using Personal Data in a way which you think an individual might think is unfair, please speak to the DPO.

5 Consent:

5.1 We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should speak to the DPO if you think that you may need to obtain consent.

5.2 Consent is required for certain mail-outs and marketing by electronic means, please check with the DPO before sending mail-outs to customers and prospective customers.

6 Personal Data must only be processed for limited purposes and in an appropriate way.

For example, if employees are told that they will be photographed for the Company's website or intranet, you should not use those photographs for another purpose (e.g., in the Company's marketing material or social media accounts) If in doubt speak to the DPO for advice and assistance.

7 Personal Data held must be adequate and relevant for the purpose.

This means not making decisions based on incomplete data. For example, when undertaking an employee's performance review, you must make sure you are using all the relevant and most up to date information about the employee.

8 Personal Data must not be excessive or unnecessary.

Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about an employee's family when it is necessary in relation to work, such as to ensure the Company is aware of an employee's childcare arrangements to assist with flexible working or contact in emergency situations.

9 Personal Data that you hold must be accurate.

You must ensure that Personal Data is complete and kept up to date. For example, if a client or third parties contact details have changed, you should update the Company's information management system OR if you are aware of inaccuracies, you must ensure they are updated or bring any inaccuracies to the attention of the DPO.

10 Personal Data must not be kept longer than necessary

The Company has a policy about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting personal data but also bear in mind when a person leaves the business then there will only be a need to retain a limited amount of information.

Please speak to the DPO for guidance on the retention periods and secure deletion.

11 Personal Data must be kept secure

You must comply with the following Company policies and guidance relating to the handling of Personal Data:

- The IT systems, e mail and internet policy
- Any risk management
- Drivers' agreement
- Complaints
- CCTV processes
- Health and safety policy
- Social media restrictions

12 Personal Data must not be transferred outside the EEA without adequate protection

If you need to transfer personal data outside the EEA (Economic European Area) please contact the DPO. For example, if you are arranging a Company trip to a country outside the EEA or working with a Customer based outside the EEA.

13 Sharing Personal Data outside the Company - dos and don'ts

Please review the following dos and don'ts:

13.1 DO share Personal Data strictly on a need-to-know basis - think about why it is necessary to share data outside of the Company - if in doubt - always ask your line manager.

13.2 DO encrypt emails which contain Critical Company Personal Data. For example, encryption should be used when sending details of an employee's ill health to external advisers or insurers; or payroll details which are likely to contain several pieces of Critical Company Personal Data to the payroll provider.

13.3 DO make sure that you have permission from your Line Manager or the DPO to share Personal Data on the Company website.

13.4 DO be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from the DPO where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from an existing customer but using a different email address).

13.5 DO be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT department.

13.6 DO NOT disclose Personal Data to the Police or other statutory agencies such as HMRC or a Local Authority without permission from the DPO.

13.7 DO NOT disclose Personal Data to third party contractors without permission from the DPO. This includes, for example, sharing Personal Data with an external marketing team to carry out a marketing campaign.

14 Sharing Personal Data within the Company

14.1 Sharing Personal Data: This section applies when Personal Data is shared within the Company. It also applies when Personal Data is shared within the Company Group.

14.2 Need to know basis: Personal Data must only be shared within the Company on a "need to know" basis.

14.3 Client files should be locked down to the Staff who need to access the information for business purposes and wider access granted only to persons with appropriate authority. If you are unsure whether a person has appropriate authority speak to the DPO.

Examples of internal sharing which are likely to comply with the GDPR:

e.g. liaising with a colleague in accounts to check whether the client has paid their bill.

Examples of internal sharing which are unlikely to comply with the GDPR:

e.g. recording an interview or telephone call without the other person knowing, leaving handover notes on a colleague's desk while they are away, using your personal mobile device without the Company's consent.

15 Individuals' rights in their Personal Data

People have various rights in their information. You must be able to recognise when someone is exercising their rights so that you can refer the matter to the DPO.

Individual's rights: Please let the DPO know if anyone (either for themselves or on behalf of another person, such as a solicitor):

15.1 wants to know what information the Company holds about them;

15.2 asks to withdraw any consent that they have given to use their information;

15.3 wants the Company to delete any information;

15.4 asks the Company to correct or change information (unless this is a routine updating of information such as contact details, which falls within your role and authorised access);

15.5 asks for electronic information which they provided to the Company to be transferred back to them or to another organisation;

15.6 wants the Company to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the Company; or

15.7 objects to how the Company is using their information or wants the Company to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

16 Requests for Personal Data (Subject Access Requests)

16.1 The right to request Personal Data: One of the most exercised rights mentioned in paragraph 0 above is the right to make a Subject Access Request. Under this right people are entitled to request a copy of the Personal Data which the Company holds about them and to certain supplemental information.

16.2 Form of request: Subject Access Requests do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid Subject Access Request. You must always immediately let the DPO know when you receive any such requests.

16.3 If you receive a Subject Access Request: Receiving a Subject Access Request is a serious matter for the Company and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so.

17 Disclosure: When a Subject Access Request is made, the Company must disclose all of that person's Personal Data to them which falls within the scope of the request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a Subject Access Request. However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to money laundering or fraud prevention.

18 Breach

A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

19 Criminal Offence

A member of Staff who deliberately or recklessly misuses or discloses Personal Data held by the Company without proper authority is also guilty of a criminal offence.

Employee Name: _____ Date: _____

Signature: _____

The ultimate responsibility for this policy lies with the Managing Director who ensures that it is given and retains the highest of priorities. This policy and its implementation will be reviewed at least annually and updated as required.

Signed by:

Ian Henderson
Managing Director
H & M Security Services Ltd

Data Protection Policy Glossary

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

[Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

General Data Protection Regulation (GDPR): The General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal Data specifically includes but is not limited to the information outlined in the Transparency Notice given to You.

Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data

relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Staff: all employees, workers, contractors, agency workers, consultants, directors, members, agency staff, temporary staff, work experience and volunteers and others.

Transparency Notices: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee Transparency Notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.