WARD SECURITY

P64. GDPR - Data Protection Policy

1. Interpretation

1.1 Definitions:

Automated Decision-Making (ADM) means when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning economic situation, personal preferences, interests, behaviour, location or movements. Profiling is an example of Automated Processing.

Company name means Ward Security Limited.

Company Personnel means all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent means 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.

Controller means 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. For the purpose of current data protection legislation, the data controller is Ward Security Holdings Ltd of Head Office, Fitted Rigging House, The Historic Dockyard, Chatham, Kent, ME4 4TZ The DPO can be contacted by email on dpo@ward-security.co.uk or telephone on 07738 219101.

Criminal Convictions Data means personal data relating to criminal convictions and offences.

Data Subject means 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) means 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) means the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance. The Ward DPO can be contacted by email on dpo@ward-security.co.uk or telephone on 07738 219101.

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

Explicit Consent means consent which requires a very clear and specific statement (that is, not just action).

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

Personal Data means 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 Special Categories of 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 Breach means 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 means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies means 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 privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process means 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 means 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.

Related Policies means the Company's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data, available on request: [P6 Data Protection Policy – CCTV Digital, P40 Data Protection Policy – CCTV Video Tape, P28 Computer Systems Usage Policy, P29 Computer Backup Policy, P63 GDPR – HR Data Policy, P56 IT Security Policy].

Special Categories of Personal Data means 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.

2. Introduction

2.1 This Policy/Privacy Standard sets out how Ward Security Limited ("we", "our", "us", "the Company") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

2.2 This Policy/Privacy Standard applies to Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

3. Scope

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

3.2 The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies.

4. Personal data protection principles

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

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

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

4.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

4.1.4 Accurate and where necessary kept up to date (Accuracy).

4.1.5 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).

4.1.6 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).

4.1.7 Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

4.1.8 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).

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

5. Lawfulness, fairness, transparency

5.1 Lawfulness and fairness

5.2 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.3 The GDPR allows Processing for specific purposes, some of which are set out below:

5.3.1 the Data Subject has given his or her Consent;

5.3.2 the Processing is necessary for the performance of a contract with the Data Subject;

5.3.3 to meet our legal compliance obligations;

5.3.4 to protect the Data Subject's vital interests; or

5.3.5 to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

5.4 Consent

5.5 A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

5.6 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing.

5.7 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured.

5.8 Transparency (notifying data subjects)

5.9 The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was

collected directly from Data Subjects or from elsewhere. We will provide such information through appropriate Privacy Notices.

6. Purpose limitation

6.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

6.2 We may, for example process Personal Data in the following ways:

6.2.1 to carry out activities connected with a contract including where relevant, its termination;

6.2.2 to monitor diversity and equal opportunities;

6.2.3 to monitor and protect the security (including network security) of Ward Security Limited, of our staff, customers and others by way of visual and audio recording inside vehicles or external CCTV filming and monitoring;

6.2.4 to monitor and protect the health and safety of our staff, customers and third parties (again this may include by way of visual and audio recording inside vehicles or external CCTV filming and monitoring);

6.2.5 paying tax and national insurance;

6.2.6 to comply with relevant legislation including health and safety law and other laws which affect us;

6.2.7 to answer questions from insurers in respect of any insurance policies;

6.2.8 running our business and planning for the future;

6.2.9 the prevention and detection of fraud or other criminal offences;

6.2.10 to defend Ward Security Limited in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure;

6.2.11 to meet our contractual obligations to provide security services (including CCTV monitoring and recording on clients' behalf);

6.2.12 to obtain relevant information via cookies. When browsing the website (www.ward-security.co.uk) the following information is collected via cookies; IP address, web browser type, geographic location, duration of visits, links or resources accessed and pages visited and response times; and.

6.2.13 to engage individuals to provide services to us as a service provider.

7. Data minimisation

7.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

7.2 We will ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

8. Accuracy

8.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9. Storage limitation

9.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.2 We will not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

9.3 The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

10. Security integrity and confidentiality

10.1 Protecting Personal Data

10.2 Personal Data will be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

10.3 Personal data securely stored in the cloud and other hosted systems in ISO27001 accredited data centres.

10.4 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

10.5 We must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

10.5.1 Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

10.5.2 Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

10.5.3 Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

10.6 Reporting a Personal Data Breach

10.7 The GDPR requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

10.8 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

11. Transfer limitation

11.1 The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. Organisations transfer Personal Data originating in one country across borders when they transmit, send, view or access that data in or to a different country.

11.2 We will only transfer Personal Data outside the EEA if one of the following conditions applies:

11.2.1 the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures

an adequate level of protection for the Data Subjects' rights and freedoms;

11.2.2 appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

11.2.3 the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

11.2.4 the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

Data Subject's rights and requests

11.3 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

11.3.1 withdraw Consent to Processing at any time;

11.3.2 receive certain information about the Data Controller's Processing activities;

11.3.3 request access to their Personal Data that we hold;

11.3.4 prevent our use of their Personal Data for direct marketing purposes;

11.3.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

11.3.6 restrict Processing in specific circumstances;

11.3.7 challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

11.3.8 request a copy of an agreement under which Personal Data is transferred outside of the EEA;

11.3.9 object to decisions based solely on Automated Processing, including profiling (ADM);

11.3.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

11.3.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

11.3.12 make a complaint to the supervisory authority; and

11.3.13 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

12. Accountability

12.1 The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

12.2 The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:

12.2.1 appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

12.2.2 implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

12.2.3 integrating data protection into internal documents including this Privacy Standard, Related Policies or Privacy Notices;

12.2.4 regularly training Company Personnel on the GDPR, this Privacy Standard and Related Policies and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

12.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

12.3 Record keeping

12.4 The GDPR requires us to keep full and accurate records of all our data Processing activities.

12.5 These records will include, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

12.6 Training and audit

12.7 We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

12.8 Privacy By Design and Data Protection Impact Assessment (DPIA)

12.9 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

12.10 Data controllers must also conduct DPIAs in respect to high risk Processing.

12.11 Automated Processing (including profiling) and Automated Decision-Making

12.12 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

12.12.1 a Data Subject has Explicitly Consented;

12.12.2 the Processing is authorised by law; or

12.12.3 the Processing is necessary for the performance of or entering into a contract.

12.13 A DPIA will be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

12.14 Direct marketing

12.15 We are subject to certain rules and privacy laws when marketing to our customers and will explicitly offer the Data Subjects the right to opt out in an intelligible manner so that it is clearly distinguishable from other information.

12.16 A Data Subject's objection to direct marketing will be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

12.17 Sharing Personal Data

12.18 Generally we will not share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

13. Changes to this Privacy Standard

13.1 We reserve the right to change this Privacy Standard at any time so please check back regularly to obtain the latest copy of this Privacy Standard. We last revised this Privacy Standard on 15 May 2019.

13.2 This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where the Company operates.