DATA PROTECTION POLICY- ADNET PRECISION ENGINEERING LIMITED

1. Interpretation

1.1 Definitions:

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

Automated Processing: 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 that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

Company name: Adnet Precision Engineering Limited (company number 05094023) of Unit B1, Nexus Court Hurricane, Road, Gloucester Business Park, GL3 4AG.

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

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, signify agreement to the Processing of Personal Data relating to them.

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 UK GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

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. A DPIA should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): either of the following:

a) the person required to be appointed in specific circumstances under the UK GDPR; or

b) where a mandatory DPO has not been appointed, a data privacy manager or other voluntary appointment of a DPO or the Company data privacy team with responsibility for data protection compliance.

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

UK GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK 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 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: 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 Notices (also referred to as Fair Processing Notices) or Privacy Policies: 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:

a) general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or

b) stand-alone, one-time privacy statements covering Processing related to a specific purpose.

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.

Special Categories of 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.

2. Introduction

2.1 This Data Protection Policy sets out how Adnet Precision Engineering Limited ("we", “us”, “our”) handle the Personal Data of our customers, prospective customers, suppliers, employees, workers, business contacts and other third parties.

2.2 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject (“you”, “your”).

2.3 Company Personnel must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. Data protection is the responsibility of everyone within the Company and this Data Protection Policy sets out the processes and procedures to be followed when handling Personal Data to enable the Company to comply with applicable law. Compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy may result in disciplinary action.

2.4 This Data Protection Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

3. Scope of Policy and when to seek advice on data protection compliance

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain trust and 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 ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

3.3 The DPO is also responsible for overseeing this Data Protection Policy. That post is held by Caroline Day, and they can be reached at *info@adnetprecision.co.uk*.

3.4 Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed.

4. Personal data protection principles

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

(a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);
(b) collected only for specified, explicit and legitimate purposes (purpose limitation);
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);
(d) accurate and where necessary kept up to date (accuracy);
(e) 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);
(f) 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);

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

5. Lawfulness, fairness and transparency

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

5.2 The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

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

(a) the Data Subject has given their Consent;
(b) the Processing is necessary for the performance of a contract with the Data Subject;
(c) to meet our legal compliance obligations;
(d) to protect the Data Subject's vital interests; or
(e) to pursue our legitimate interests (or those of a third party) 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;

6. Consent

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

6.2 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.3 A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.4 When processing necessary Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

7. Transparency (notifying Data Subjects)

7.1 The UK GDPR requires a Controller, us, to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

7.2 Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

7.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we will provide the Data Subject (so far as is necessary) with all the information required by the UK GDPR as soon as reasonable after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

8. Purpose limitation

8.1 Personal Data will be collected only for specified, explicit and legitimate purposes. It will not be further Processed in any manner incompatible with those purposes, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use Personal Data for a new unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

9. Data minimisation

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

9.2 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.

10. Accuracy

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

10.2 We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11. Storage limitation

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

11.2 The Company will take into account the following circumstances when determining the appropriate retention period for Personal Data:

(a) the amount, nature and sensitivity of the Personal Data retained;

(b) The potential risk of harm from unauthorised use or disclosure of Personal Data;

(c) The purpose for which the Personal Data is held; and

(d) The applicable legal requirements.

11.3 We will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require.

12. Security integrity and confidentiality

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

12.2 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 where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

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

(a) Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;

(b) Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

12.4 We must comply with and not attempt to circumvent the administrative, physical and technical safeguards that we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

13. Reporting a Personal Data Breach

13.1 The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

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

14. Transfer limitation

14.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. Personal Data originating in one country is transferred across borders when you transmit, send, view or access that data in or to a different country.

14.2 If Personal Data is transferred outside the UK, we will reasonably endeavour or reasonably procure that a similar degree of protection is afforded to it by implementing as far as is possible and necessary, appropriate safeguards.

15. Data Subject's rights and requests

15.1 A Data Subject has rights when it comes to how we handle their Personal Data. These include rights to:
- (a) withdraw Consent to Processing at any time;
- (b) receive certain information about the Controller's Processing activities;
- (c) request access to their Personal Data that we hold (including receiving a copy of their Personal Data);
- (d) prevent our use of their Personal Data for direct marketing purposes;
- (e) 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;
- (f) restrict Processing in specific circumstances;
- (g) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- (h) make a complaint to us and subsequently to the supervisory authority, the Information Commissioner's Office;

16. Accountability

16.1 We shall maintain adequate resources and controls in place to ensure and to document UK GDPR compliance. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

17. Training and audit

17.1 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.

18. Automated Processing (including profiling) and Automated Decision-Making

18.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:
- (a) a Data Subject has Explicitly Consented;
- (b) the Processing is authorised by law; or
- (c) the Processing is necessary for the performance of or entering into a contract.

18.2 If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed. However, the Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

19. Direct marketing

19.1 We may use Personal Data for marketing purposes.

19.2 We are subject to certain rules and privacy laws when engaging in direct marketing to our customers and prospective customers (for example when sending marketing emails or making telephone sales calls).

19.3 Whilst we will usually obtain your Consent for electronic direct marketing, we may send marketing texts or emails without your consent if:
- (a) We have obtained the contact details in the course of a sale to that person.
- (b) We are marketing a similar product or service.
- (c) We have given the person an opportunity to opt out of marketing when first collecting the details and in every subsequent marketing message.

19.4 You have the right to object to direct marketing communications at any time by contacting the DPO.

19.5 A Data Subject's objection to direct marketing must always be promptly honoured. If a customer opts out of marketing 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.

20. Sharing Personal Data

20.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

20.2 We may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;
(b) the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;
(c) the transfer complies with any applicable cross-border transfer restrictions; and
(d) a fully executed written contract that contains UK GDPR-compliant third party clauses has been obtained.

21. Website Privacy Policy

21.1 Our Privacy Policy can be found using the following link- *Privacy Policy - Adnet Precision*. The Privacy Policy should be read in connection with this Data Protection policy, especially with regard to how information is collected and kept on our website and the limitation of our liability for third party links.

22. Changes to this Data Protection Policy

22.1 We keep this Data Protection Policy under regular review.

22.2 This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

Adnet Precision Engineering- Data Protection Policy- September 25.