John Aynsley

(ARCHITECTURAL METALWORK) LIMITED

DATA PROTECTION ACT AND GDPR POLICY

INTRODUCTION

1 Background

1.1 John Aynsley (Architectural Metalwork) Ltd needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly'.

1.2 Personal data at John Aynsley (Architectural Metalwork) Ltd can include employees (present, past and prospective), clients, customers, contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic or other form.

1.3 Irrespective of how information is collected, recorded and processed person-identifiable information must be dealt with properly to ensure compliance with the Data Protection Act (DPA) 1998 and the General Data Protection Regulations (GDPR).

1.4 The DPA requires us to comply with the eight Data Protection Principles (see Appendix A below) and to notify the Information Commissioner about the data that we hold and why we hold it. This is a formal notification and is renewed annually.

1.5 The DPA gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances to ask us to stop using it and to seek damages where we are using it improperly.

1.6 The lawful and correct treatment of person-identifiable information by us is paramount to the success of the organisation and to maintaining the confidence of our clients, suppliers, contractors and employees. This policy will help us ensure that all person-identifiable information is handled and processed lawfully and correctly.

Data Protection Act and GDPR principles

1.7 John Aynsley (Architectural Metalwork) Ltd has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security.

1.8 The aim of this policy is to outline how John Aynsley (Architectural Metalwork) Ltd meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The

obligations within this policy are principally based upon the requirements of the Data Protection Act 1998 and GDPR, as the key legislative and regulatory provisions governing the security of person-identifiable information.

1.9 Other relevant legislation and guidance referenced and to be read in conjunction with this policy, is outlined together with a brief summary at Appendix B.

2. What information is covered?

2.1 Personal data within the respective legislative and regulatory provisions covers 'any data that can be used to identify a living individual either directly or indirectly'. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

3. Policy statement

3.1 This document defines the data protection policy for John Aynsley (Architectural Metalwork) Ltd. It applies to all person-identifiable information obtained and processed by the organisation and its employees. It sets out:

- the organisation's policy for the protection of all person-identifiable information that is processed
- establishes the responsibilities (and best practice) for data protection
- references the key principles of the Data Protection Act 1998 and GDPR.

4. Principles

4.1 The objective of this policy is to ensure the protection of John Aynsley (Architectural Metalwork) Ltd 's information in accordance with relevant legislation, namely:

- To ensure notification; Annually notify the Information Commissioner about our use of person-identifiable information.
- To ensure professionalism; All information is obtained, held and processed in a professional manner in accordance with the eight principles of the Data Protection Act 1998 and the provisions of the GDPR.
- To preserve security; All information is obtained, held, disclosed and disposed of in a secure manner.
- To ensure awareness; Provision of appropriate training and promote awareness to inform all employees of their responsibilities.
- Data Subject access; Prompt and informed responses to subject access requests.

4.2 The policy will be reviewed periodically by our Directors. Where review and update is necessary due to legislative changes this will be done immediately.

4.3 In accordance with our equality and diversity policy statement, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.

5. Scope of this policy

5.1 This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need to know basis.

5.2 The procedures cover all person identifiable information whether electronic or paper which may relate to clients, customers, employees, contractors or other stakeholders and third parties about whom we hold information.

6. Policy

6.1 John Aynsley (Architectural Metalwork) Ltd obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:

- staff records and administrative records
- contractual obligations with clients, customers and contractors.
- complaints and requests for information.

6.2 Such information may be kept in either computer or manual records. In processing such personal data we will comply with the data protection principles within the Data Protection Act 1998.

7. Data protection responsibilities

Overall responsibilities

7.1 John Aynsley (Architectural Metalwork) Ltd is responsible for data security and is known as the 'data controller' and permits the organisation's staff to use computers and relevant filing systems (manual records) in connection with their duties. The Company has legal responsibility for the notification process and compliance of the Data Protection Act 1998.

7.2 John Aynsley (Architectural Metalwork) Ltd whilst retaining their legal responsibilities has delegated data protection compliance to the Data Protection Officer.

7.3 The Data Protection Officer's responsibilities have been allocated to the Company's administration staff.

Data Protection Officer's (DPO) responsibilities

7.4 The Data Protection Officer's responsibilities include:

- ensuring that the policy is produced and kept up to date
- ensuring that the appropriate practice and procedures are adopted and followed by the company.
- provide advice and support to the Directors on data protection issues within the organisation
- ensure data protection notification with the Information Commissioner's Office is reviewed, maintained and renewed annually for all use of person-identifiable information.
- ensure compliance with individual rights, including subject access requests.

- act as a central point of contact on data protection issues within the organisation.
- implement an effective framework for the management of data protection.

General responsibilities

7.6 All employees, including temporary and contract staff are subject to compliance with this policy. Under the GDPR individuals can be held personally liable for data protection breaches.

7.7 All employees have a responsibility to inform their line manager and the Data Protection Officer of any new use of personal data, as soon as reasonably practicable after it has been identified.

7.8 All employees will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the Data Protection Officer.

7.9 Employees must follow the subject access request procedure (see Appendix C below).

8. Monitoring

8.1 Compliance with this policy will be monitored by the Data Protection Officer.

9. Validity of this policy

9.1 A formal review shall take place upon an annual basis.

Appendix A - Data Protection Act 1998 - Data protection principles

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix B – Summary of relevant legislation and guidance

General Data Protection Regulations (GDPR)

A legal basis must be identified and documented before personal data can be processed. 'Controllers' and 'Processors' will be required to document decisions and maintain records of processing activities.

Freedom of Information Act 2000

This Act gives individuals rights of access to information held by public authorities.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the "Interception of Communications Act 1985". The aim of the Act was to modernise the legal regulation of interception of communications, in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area. The Act allows disclosure of person-identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose person-identifiable information and responsibility for disclosure rests with the organisation holding the information.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This Act allows employers to intercept and record communications in certain prescribed circumstances for legitimate monitoring, without obtaining the consent of the parties to the communication.

Appendix C– Subject access request process

- Request received for personal information or other data (in person, by telephone, electronically or in writing)
- Check request, is all required information provided.
- Report to Data Protection Officer
- Data Protection Officer checks to see if Data is held.
- Data Protection Officer reports to Director for permission to release data
- Data Protection Officer Checks to see if a data release exemption is in place.
- Data Protection Officer Checks to see if a data release exemption is involved.
- Remove all third party information
- Release data or inform applicant as to reason for no data release