The Fabulous Fascia Company Ltd

COMPANY DATA PROTECTION POLICY

Adopted by the company on 24th May 2018
Policy to be reviewed in May 2019

Definitions

“Data Protection Legislation” means the Data Protection Act (1998), the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003, and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the processing of personal data, including, where applicable, the guidance and codes of practice issued by the Information Commissioner’s Office (ICO).

The Data Protection Legislation (“the Legislation”) is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully, and that where necessary the privacy of individuals is respected. During the course of the activities of The Fabulous Fascia Company Limited (“the Company), the Company’s Director (“we”) will collect, store and process personal data about our employees, sub-contractors, clients as well as activities, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the Company. This policy sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

The Managing Director is responsible for ensuring compliance with the Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Managing Director.

Processing personal data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action.

Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.

Personal data is data relating to a living individual. It includes employee data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered.

Personal data can be factual (e.g. a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Employees and others who process data on behalf of the Company should assume that whatever they do with personal data will be considered to constitute processing. Individuals should only process data if there is a lawful basis to do so. If there is any doubt, individuals should contact the Data Protection Compliance Manager before processing personal data..

Compliance with the Legislation

Employees and others who process data on our behalf have a responsibility for processing personal data in accordance with the Legislation. Anyone who has responsibility for processing personal data must ensure that they comply with the data protection principles in the Legislation. These state that personal data must:

- Be obtained and used fairly and lawfully;
- Be obtained for specified lawful purposes and used only for those purposes;
- Be adequate, relevant and not excessive for those purposes;
- Be accurate and kept up to date;
- Not be kept for any longer than required for those purposes;
- Be used in a way which complies with the individual's rights (this includes rights to prevent the use of personal data which will cause them damage or distress, to prevent use of personal data for direct marketing, and to have inaccurate information deleted or corrected);
- Be protected by appropriate technical or organisational measures against unauthorised access, processing or accidental loss or destruction;
- Not be transferred outside the European Economic Area unless with the consent of the data subject or where the country is determined to have adequate systems in place to protect personal data.

Monitoring the use of personal data

We are committed to ensuring that this data protection policy is put into practice and that appropriate working practices are being followed. To this end the following steps

will be taken:

- Any employees who deal with personal data are expected to be aware of data protection issues and to work towards continuous improvement of the proper processing of personal data;
- Employees who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored;
- All employees must evaluate whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure inaccurate, excessive or out of date data is disposed of in accordance with this policy;
- Spot checks may be carried out;
- An annual report on the level of compliance with, or variance from, good data protection practices will be produced by the Managing Director. Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

Handling personal data and data security

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing or unauthorised disclosure. Manual records relating to Company members, staff or other individuals will be kept secure in locked cabinets. Access to such records will be restricted. Computer files should be password protected.

We will ensure that staff and members who handle personal data are adequately trained and monitored.

We will take particular care of sensitive data, and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out below).

Security policies and procedures will be regularly monitored and reviewed to ensure data is being kept secure.

Where personal data needs to be deleted or destroyed, adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and backup files, and the physical destruction of manual files. Particular care should be taken over the destruction of sensitive data.

All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed.

Any agent employed to process data on our behalf will be bound to comply with this data protection policy by a written contract.

The rights of individuals

The Legislation gives individuals certain rights to know what data is held about them and what it is used for. In principle everyone has the right to see copies of all personal data held about them. There is also a right to have any inaccuracies in data corrected or erased. Data subjects also have the right to prevent the processing of their data for direct marketing purposes.

Any request for access to data under the Legislation should be made to the Managing Director in writing. In accordance with the Legislation we will ensure that written requests for access to personal data are complied with within 30 days of receipt of a valid request.

When a written data subject access request is received, the data subject will be given:

a) A description of the personal data

b) A description of the purposes for which it is being processed

c) A list of those people and organisations to whom the data may be disclosed

d) A copy of the information in an intelligible form.

Sensitive data

Although we cannot foresee having this information, we will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards can be put in place. Sensitive data means data consisting of information relating to an individual's:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal offences

Sickness records are likely to include sensitive data and as such should only be held if the explicit consent of each employee is obtained, or if one of the other conditions for processing sensitive data is satisfied.

Storage of data and records

All data and records will be stored in accordance with the security arrangements of the Legislation and in the most convenient and appropriate location, having regard to the period of retention required and the frequency with which access will be made to the record.

Data and records which are active should be stored in the most appropriate place for their purpose commensurate with security requirements.
Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose.

The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.

Any data file or record which contains personal data of any form can be considered as confidential in nature.

Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Legislation, which requires that personal data processed for any purpose 'shall not be kept for longer than is necessary for that purpose.' All groups are required to have regard to the Guidelines for Retention of Personal Data (Appendix A).

Any data that is to be disposed of must be safely disposed of, for example by shredding. The company has its own shredder.

Special care must be given to disposing of data stored in electronic media, for example, personal computers or laptops.

Information security

Information security involves preserving confidentiality, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users.

Information security is the responsibility of every member of staff, using data on, but not limited to, Company information systems.

Our IT systems may only be used for authorised purposes. We may monitor the use of our systems from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

We will ensure information security by:

- Ensuring appropriate software security measures are implemented and kept up to date;
- Making sure that only those who need access have that access;
- Not storing information where it can be accidentally exposed or lost;
- Making sure that if information has to be transported, it is done so safely using encrypted devices or services.

Access to systems on which information is stored must be password protected. Passwords must not be disclosed to others. If you have a suspicion that your password has been compromised, you must change it.

You must ensure that any personally owned equipment which has been used to store or process Company data is disposed of securely. Software on personally owned devices must be kept up to date.

Unsecured wi-fi must not be used to process Company data.

Data breaches

Every care is taken to protect the data we hold. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties.

We will strive to contain any breaches, to minimise the risks associated with the breach, and pledge to consider what action is necessary to secure personal data and prevent any further breach.

(A). Types of breach

An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects. An incident includes, but is not limited to:

- Loss or theft of personal data or the equipment on which the data is stored, e.g. laptop, smartphone, memory stick or paper record;
- Theft or failure of equipment on which personal data is stored;
- Unauthorised use of or access to personal data;
- Attempts to gain unauthorised access to personal data;
- Unauthorised disclosure of personal data;
- Website defacement;
- Hacking attack.

(B). Reporting an incident

Any person using personal data on behalf of the Company is responsible for reporting data breach incidents immediately to the Managing Director. The report should contain the following details:

- Date and time of discovery of the breach;
- Details of the person who discovered the breach;
- The nature of the personal data involved;
- How many individuals' data is affected.

(C). Containment and recovery

The Managing Director will first ascertain if the breach is still occurring. If so,

appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Consideration will be given as to whether the police should be informed. Advice from appropriate experts will be sought if necessary. A suitable course of action will be taken to ensure a resolution of the breach.

(D). Investigation and risk assessment

An investigation will be carried out without delay, and where possible within 24 hours of the breach being discovered. The Managing Director will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those consequences are, and how likely they are to occur.

The investigation will take into account the following:

- The type of data involved and its sensitivity;
- The protections in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to illegal or inappropriate use;
- Who the data subjects are, how many are involved, and the potential effects on them;
- Any wider consequences.

(E). Notification

The Managing Director will decide with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case by case basis. Consideration will be given to notifying the Information Commissioner if a large number of people are affected or the consequences for the data subjects are very serious. Guidance on when and how to notify the ICO is available on their website: www.ico.org.uk/media/1536/breach_reporting.pdf

Notification to the data subjects whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the nature of the data involved. Specific and clear advice will be given on what they can do to protect themselves and what has already been done to mitigate the risks.

The Data Protection Compliance Manager (who will be the Managing Director) will keep a record of all actions taken in respect of the breach.

(F). Evaluation and response

Once the incident is contained, the Managing Director will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring.

Complaints

We take privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact the Managing Director:

The Fabulous Fascia Co. Ltd
8 Frietuna Road
Frinton-on-Sea
Essex

Tel. 01255 678192
Email info@fabulousfascia.co.uk

We will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation. We will keep you informed of the progress of our investigation and the outcome. If you are not satisfied with the outcome, you may wish to contact the Information Commissioner's Office at https://ico.org.uk/concerns.

When any complaint is received by us, the Managing Director will arrange for an investigation as follows:

- A record will be made of the details of the complaint;
- Consideration will be given as to whether the circumstances amount to a breach of the Legislation and action will be taken in accordance with the Data Breach procedure;
- The complainant will be kept informed of the progress of the compliant and of the outcome of the investigation;
- At the conclusion of the investigation, the Managing Director will reflect on the circumstances and recommend any improvements to systems or procedures.

Changes to this policy

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Appendix 1 Guidelines for the retention of Data

This is not an exhaustive list. If you have any queries regarding retaining or disposing of personal data, please contact the Managing Director at once.

Types of Data	Retention period
Employee data: ● Personnel files (including training records and notes of disciplinary and grievance hearings	6 years from end of employment
● Application forms/interview notes	Max year for those not subsequently employed. If employed, retain in personnel file.
● Income tax & NI returns, including correspondence with tax office	At least 6 years after end of financial year to which the records relate
● Statutory Maternity/Paternity Pay records and calculations	As above
● Statutory Sick Pay records and calculations	As above
Wages and salary records	6 years from the tax year in which generated
● Health records	6 months from date of leaving employment
● Health records where reason for termination of employment is connected with health (including stress related illness)	3 years from date of leaving employment
Client data: ● Client information on order form	10 years after installation (for the purposes of fulfilling the guarantee) 15 years for Lindab orders (ditto) 40 years for Alutec orders (ditto)

Appendix 2 Privacy Notice

The Fabulous Fascia Company Limited - Company Privacy Notice

How The Fabulous Fascia Company Ltd ("we") use your information

Your privacy is important to us. We are committed to safeguarding the privacy of your information.

Why do we collect and use your information?
We collect and use your information to fulfil our purposes as a Company. We do not share your information with others except as described in this notice.

We may like to send you information about our events, offers and activities by post, telephone, email and SMS. If you agree to being contacted in this way, please tick the relevant boxes

- ☐ Post
- ☐ Email
- ☐ Phone
- ☐ SMS

Signed_____ Date____/____/_____

The categories of information that we may collect, hold and share include:

- Personal information (such as name, telephone number, address and email address)

Storing your data

We hold your data for varying lengths of time depending on the type of information in question but in doing so we always comply with Data Protection legislation. We will contact you annually to check that the information we are holding is accurate and that you agree to us holding it.

Who do we share your information with?

We will not share your information with third parties without your consent unless the law requires us to do so.

Requesting access to your personal data

Under Data Protection legislation, you have the right to request access to information

about you that we hold. To make a request for your personal information contact the Managing Director.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

For further information on how your information is used, how we maintain the security of your information and your rights to access information we hold on you please contact the Managing Director

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

The Managing Director:-

Gary Stevens BA (Hons)
8 Frietuna Road, Frinton-on-Sea, Essex, CO13 0RY