GDPR Compliance Procedures

This document has been prepared in conjunction with the forth coming EU GDPR legislation which comes into effect on 25th May 2018. The following processes comply fully with GDPR standards and clearly outline the Company's actions with regard to personal data, legal bases and documents in use at every stage.

It is deemed in this process that Apex Engineering Solutions (The Company) is acting as the Data Controller and in that capacity we will identify the legal basis to which we will rely on so that we may process an individual's data. The basis of this will depend on the type of data held, whether personal data or sensitive data.

Source of Personal data

These are the common ways in which the Company will gain personal data.

1. Candidate uploads CV to the Company website
2. Referral
3. Agency finds individual via a job board
4. Agency finds an individual on a social networking site

Documents used

In all cases the data subject is given a GDPR compliant Registration Form (copies of which can be downloaded off the Agency website).

In 1. Form DP5A – Privacy Statement is also issued, whereas in 2,3 & 4 Form DP5B – Privacy Statement is issued.

Privacy Statement

The Privacy Statement clearly outlines the key areas;

- Purpose of Processing and legal basis
- Categories of data - what information is gathered, ie Name, Contact details, other specific data
- Legitimate Interest is the basis for gathering the data
- Recipient of data - Whether this information will be shared with a third party
- Data Retention – The period of time that the data will be held for. *Note under the Conduct of Employment Agencies and Employment Business Regulations 2003 an Agency is required to keep data for a minimum of 12 months.*
- The Individuals Rights – listed and explained
- Source of the personal data – where it came from (this only applies to 2,3 & 4)

Legal bases

The Company will only process data where it has a legal basis for doing so. For the purpose of carrying out the role of a Recruitment Consultancy personal data is gained and held through Legitimate Interest as the Company is providing work finding services and the individual is seeking employment. Although legitimate interest is the initial basis for holding personal data the Company will not rely on this lawful basis and will endeavour to gain Written Consent as soon as possible.

The Company will review the personal data it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date.

Written Consent
The individual will be asked to complete a consent form (download available on the Company website), which will be uploaded to their personal record card on the inhouse database.

Privacy by design and default
The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all processing activities. The includes implementing measures such as;

- Data minimisation
- Pseudonymisation
- Anonymization
- Cyber security

Security of Personal data
All personal data is held digitally on a secure database. The Data is backed up remotely to a third party using end to end encryption. Some files are held in paper form in locked filing cabinets.

Only Company employees have access to the data held on the database and this is not shared with any third parties, apart from the required IT processing and backing up functions.

Third Parties
All third party providers have been audited and compliance checks have taken place to ensure GDPR standards are being met and all data is processed in a secure fashion.

Data Breaches
An Incidence response process has been defined whereby any data breach will be highlighted immediately and the Data Protection Representative will be contacted and a plan of action will be put in place to determine the nature and severity of the breach.

Where the Company establishes that a personal data breach has taken place, the Company will take steps to contain and recover the breach. Where a personal breach is likely to result in a risk to the rights and freedoms of any individual the Data Protection Representative will notify the ICO.

Where the Company has identified a personal data breach resulting in a high risk to the rights and freedoms of any individual the Company shall tell all affected individuals without undue delay.

The Company will not be required to inform individuals about the personal data breach where:

- The Company has implemented appropriate technical and organisational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorised to access it, such as encryption.
- The Company has taken subsequent measures, which ensures that the high risk to the rights and freedoms of the individual is no longer likely to materialise.

- It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

Contact Details

For further the detail on Data Protection or GDPR compliance issues please contact **Tim Homer** (**Certified EU GDPR Foundation and Practitioner)** who is the Data Protection Representative for the Company. He is contactable on t.homer@apexes.co.uk Tel 0113 8631471.