Prospect Site Services LTD.

Electrical & mechanical Temporary Services

Data Protection Policy

INTRODUCTION

Prospect Site Services Ltd is committed to preserving the privacy of its clients, customers, suppliers and employees and to complying with the Data Protection Act 1998 and 2003 and the General Data Protection Regulations 2016 which come into force 25 May 2018. The GDP Regulations consolidate, develop and enhance the Data Protection Acts. The Requirements of the GDP Regulations are being subsumed into the company practices and procedures and are being introduced to ensure compliance as quickly as possible.

To achieve this commitment, information about our customers, employees and other clients and contacts must be collected and used fairly, stored safely and not unlawfully disclosed to any other person. We are also committed to ensure that as far as is possible and practical, that our electronic systems for storage are protected, secured and penetration tested at regular intervals. We will ensure that we only collect such data that is required and pertinent to the delivery of the service/s that we provide. We will store information for periods which are justifiable for the service delivery and will ensure confidential and safe destruction of data that may no longer be held beyond justifiable periods. Information that is already in the public domain is currently exempt from the Data Protection Act 1998 and 2000. It is company policy to make as much information public as possible and in particular the following information will be available to the public.

Names of our Director.
Photographs of key staff i.e. members of the Company and other managers.
List of key staff.
Where necessary we will implement changes and/or enhancements as required by the GDPRegulations

PRINCIPLES

The Company, its staff and others who process or use any personal information must ensure that they follow the data protection principles set out in the Data Protection Act 1998 and the General Data Protection Regulations 2016. Broadly these are that personal data shall:

Be obtained and processed fairly and lawfully and with consent

Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

Be adequate, relevant and not excessive for those purposes for which it is collected, processed and stored

Be accurate and kept up to date.
Not be kept longer than is necessary for that purpose.
Be processed in accordance with the data subject rights.
Be kept safe from unauthorised access, accidental loss or destruction.

Be available for lawful inspection
Be amended if the data is demonstrated to be inaccurate or excessive for purpose
Not be transferred to a country outside the European Economic area, unless
that country has equivalent levels of protection for personal data.

Personal Data

Personal data covers both facts and opinions about an individual where that data identifies an individual. For example, it includes information necessary for employment such as the member of staff's name and address and details for payment of salary. Personal data may also include sensitive personal data as defined in the Act/GDPR.

Processing of Personal Data

Consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with appropriate consent.
If a person wishes to revoke or change consent, they must agree a specific agreement on how their data is to be processed with the Data Processor and/or Data Controller.
The company may process some personal data for direct marketing and awareness purposes, data subjects have to opt into these activities, which must be respected, i.e. consent will be sought before making direct contact.

Sensitive Personal Data

The company may, from time to time, be required to process sensitive personal data.
Sensitive personal data includes data relating to medical information, gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings. Care shall be exercised when such personal data/information is being processed to ensure that the processing is lawful and justified. Reference should be made to the Data Controller before processing sensitive personal data.

Rights of Access to Information

Data subjects have the right of access to information held by the company, subject to the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000 and the GDP Regulations. Any data subject wishing to access their personal data should put their request in writing to the company Data Controller. The Company will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, within 30 days for access to records and 21 days to provide a reply to an access to information request. The information will be imparted to the data subject as soon as is reasonably possible after it has come to the company's attention and in compliance with the relevant Acts.

Exemptions

Certain data is exempted from the provisions which includes the following: -

- National security and the prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Company including Safeguarding and prevention of terrorism and radicalisation

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the Data Controller.

The company will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the Data processor/Data Controller of any changes to information held about them. Data subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

Enforcement

If an individual believes that the company has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act and or GDPR the member of staff should utilise the company grievance procedure and should also notify the Data Processor/Data Controller.

Data Security

The company will take appropriate technical and organisational steps to ensure the security of personal data.

All staff will be made aware of this policy and their duties under the Act and the General Data Protection Regulations.

The Company and therefore all staff, are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems and be encrypted when transported offsite. Other personal data may be for publication or limited publication within the Company therefore having a lower requirement for data security. We will ensure that access to data held will only be permitted on a “need to know” basis to identified staff.

Attention is also drawn to the existence of the Information and Computing Technology (ICT) Use Policy, which provides more specific information on digital data protection within the policy, and best practice guides that are published and shall be adhered to.

External Processors

The company will ensure that data processed by external processors, for example, service providers, Cloud services including storage, web sites etc. are compliant with this policy and the relevant legislation.

Secure Destruction

When data held in accordance with this policy is destroyed, it will be destroyed securely in accordance with best practice at the time of destruction and destruction audit trail provided and documented.

Retention of Data

Documents Control Reference: Corp 007:1.0

The company may retain data for differing periods of time for different purposes as required by statute or best practices. Retention times are specified and included within the processes and manuals. Other statutory obligations, legal processes and enquiries may also necessitate the retention of certain data.

FURTHER PRACTICAL IMPLICATIONS

We will ensure that we undertake penetration testing at reasonable intervals to safeguard and protect the data that we hold.

We will not use any information or data collected for the purposes of marketing or general communication (e.g. newsletters) for which explicit permission/authorisation has not been given.

Staff will not “copy in” emails to a primary recipient where the address of the other recipients is exposed where permission has not been provided.

Staff shall be vigilant at all times when collection, processing, storing and using information/data to ensure adherence and eliminate breaches of data security. Any identified potential breach or weakness that might lead to a breach shall be reported to the Data Controller.

The Company will not release staff or client data to third parties except to relevant statutory bodies. In all other circumstances the Company will obtain the consent of the individuals concerned before releasing personal data.

RESPONSIBILITIES

Managing/Director

The Managing Director is responsible for the oversight, implementation, communication and scrutiny of adherence to this policy and ensuring review at not more than annual intervals.

Data Protection Controller (DPC)

The nominated Data Protection Controller has operational responsibility for the implementation of this policy and for ensuring that any identified breaches of protection or security are reported to the Information Commissioner's Office within 72 hours of initial identification. The DPC will be responsible for initiating and supervising the corrective actions and for implementing preventative actions to eliminate further breaches of security

Managers/Supervisors

Managers are responsible for ensuring that staff are aware of and abide by this policy.
Managers are responsible for ensuring the secure collection, storage and processing of any paper (hard copies) of personal information and shall ensure that access to such personal information is restricted to authorised and nominated staff and kept in secure and locked conditions.

All Staff

All staff are responsible for ensuring that any personal data which they hold is kept securely and that personal information is not disclosed in any way and to any unauthorised third party.
Apprentices/Trainees/Learners and staff are responsible for ensuring that all personal data provided to the Company is accurate and up to date.

COMPLIANCE

Protection and security of data held is seen as a most important activity of the business.
Failure to comply with the data protection policy and procedures could result in disciplinary action.

REVIEW

This policy and related procedures will be reviewed and issued on at least an annual basis.

Approval for this statement

This statement was approved by the Director, Mr Chris Valentine

Signed for Prospect Site Services LTD:

Mr Chris Valentine Managing Director	C.Valentine
Date:	16th February 2021
Review Date:	16th February 2022