Contract Services Europe

Data Protection Policy

1. INTRODUCTION

This Policy sets out the obligations of DPS Contract Services ("the Company") regarding data protection and the rights of employees, contractors and job applicants in the EU ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation").

- The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, contractors, or other parties working on behalf of the Company.
- The Company places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Responsibilities of The Data Protection Officer:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all staff members and those included in this policy.
- Answering questions on data protection from staff, board members and other stakeholders.
- Responding to individuals such as clients and employees who wish to know which data is being held on them by DPS Contract Services.
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Responsibilities of the IT Manager:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

2. THE DATA PROTECTION PRINCIPLES

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

a. processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes

c. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d. accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that is inaccurate is erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. LAWFUL, FAIR, AND TRANSPARENT DATA PROCESSING

The Company will always process your personal data lawfully, fairly, and transparently, without adversely affecting your rights as the data subject.

Details on how we achieve this can be found in section 3, 4 and 7 of our Privacy notice (link to Privacy notice) and section 12 of our Records Retention Policy (link to Records Retention Policy)

4. PROCESSED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

The Company only collects and processes personal data for the specific purposes set out in Part 12 of this Policy.

Details of how we achieve this can be found in section 4 of our Privacy Notice (link to Privacy Notice)

5. ADEQUATE, RELEVANT AND LIMITED DATA PROCESSING

The Company will only collect and process personal data for, and to the extent necessary, for the specific purposes informed to data subjects as under Part 4, above.

6. ACCURACY OF DATA AND KEEPING DATA UP TO DATE

The Company ensures that all personal data collected and processed is kept accurate and up-to-date.

The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate. Further information can be found in section 5.2 and 5.3 of the Procedure for Handling of Individual rights (link)

7. TIMELY PROCESSING

The Company does not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed.

When the data is no longer required, all reasonable steps will be taken to erase it without delay and will be securely deleted in line with our Records Retention Policy (link)

8. SECURE PROCESSING

The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Further details of the data protection and organisational measures which shall be taken are provided in Parts 13 and 14 of this Policy.

9. ACCOUNTABILITY

The Company's data protection officer is responsible for the governance of personal data. This will be achieved by demonstrated by the maintenance of internal records of all personal data collection, holding, and processing.

10. PRIVACY IMPACT ASSESSMENTS

The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's data protection officer.

11. THE RIGHTS OF DATA SUBJECTS

The Regulation sets out the following rights applicable to data subjects. Under certain circumstances, by law you have:

a. The right to be informed;
b. The right of access to your personal data;
c. The right to rectification of your personal data;
d. The right to erasure of your personal data;
e. The right to restrict processing of your personal data;

f. The right to data portability;

g. The right to object to the processing of your personal data

h. Rights with respect to automated decision-making and profiling.

You can find further information on how to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, request that we transfer a copy of your personal information to another party and how to exercise your rights as a Data Subject in our Procedure for Handling of Individual Rights (link) and our Privacy Notice (link)

12. PERSONAL DATA

The following personal data may be collected, held, and processed by the Company. Personal data relates to a specific individual who may be identifiable from that data. This can include;

12.1 Information collected and processed for finding the data subject a suitable role is as follows:

- Contact information (e.g. name, postal and email addresses)
- Qualifications, skills and competencies
- CV and documents supporting data subject job applications, including references and transcripts
- Employment history
- Data Subject responses to job specific questions
- Assessment test results e.g. pre-employment medical

12.2 Information in respect to individuals that have worked for us previously or may work for us is as follows

- Passport
- In some cases, permits and visas
- DOB
- PPS number or Social Security number
- Details of job offers and placements
- Outcome of background and criminal record checks for certain roles
- In certain cases, medical information
- Financial information (including but not limited to payroll details and terms)

The above information is used to provide Company services to the data subject in our capacity as an employment business to find the data subject suitable work whether on a temporary, contract or permanent basis, based on the data subjects' requirements as set out below.

The information under 12.1 may be used as follows:

- To match the Data Subjects skills sets with job vacancies to assist in finding Data Subjects suitable positions
- To put forward Data Subjects details to the Company clients in order for Data Subject to be considered for vacancies
- To place Data Subject with our clients
- To keep Data Subject informed of available opportunities as they arise

The information under 12.2 may be used as follows:

- To establish that Data Subject has the right to work
- To undertake relevant security and criminal record checks as required by our clients
- To deal with any medical and health and safety issues relating to certain positions
- To put in place contractual arrangements and documentation once a role has been secured
- To pay the Data Subject if placed

12.3 We will ensure any use of personal data is justified using at least one of the conditions for processing. All Company staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a Privacy Notice (link).

13. DATA PROTECTION MEASURES

The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf are subject to the following when working with personal data:

a. A fully resourced and engaged data protection governance structure across the organisation supported by a suite of enforced data protection policies, processes and guidance.

14. ORGANISATIONAL MEASURES

The Company has measures in place to identify, understand and manage the risks to personal data and appropriate controls are in place to prevent, limit or contain the impact of unwanted events to personal data transmitted, stored or processed.

15. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

15.1 The Company may from time to time transfer personal data to countries outside of the EEA.

15.2 The transfer of personal data to a country outside of the EEA shall only take place with the informed consent of the relevant data subject(s) and the transfer is to a country that the European

Commission has determined that such countries ensure an adequate level of protection for personal data

16. DATA BREACH NOTIFICATION

DPS CS operates a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data

Details of how we achieve this can be found in our Personal Data Breach and Incident Handling Procedure (link)

17. DATA PROTECTION TRAINING

17.1 All staff will regularly receive data protection and information security training.

a. New joiners will receive training as part of the induction process.

b. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Completion of training is compulsory.

18. IMPLEMENTATION OF POLICY

This Policy shall be deemed effective as of 25th May 2018.