PERSONAL DATA PROTECTION POLICY

Jobs Operations Ltd. is registered in the Commercial Register with UIC: 205801153, address- Sofia 1000, 21 Lavele Str. Floor 5,tel. +359 892 040302, hereinafter referred to as Jobs Ops – collects, processes and stores your personal data under the terms of this Personal Data Protection Policy.

Legal basis and Definitions

Personal Data Protection Policy (the Policy) is based on the Personal Data Protection Act (PDPA), its regulations and the GDPR (Regulation 2016/679 of the European Parliament and of the Council).
Personal data is any information through which individuals (Data subjects) can be identified.
This Policy applies to data subjects within the meaning of GDPR and PDPA, and the information is processed by Jobs Ops in its capacity of Controller and Personal Data Processor.
The data processing aims primarily the provision of information services and resources, and the process requires identification of the persons involved therein.
Personal data are processed on the basis of:

– consent of the Data Subject;

– subject to the General Terms and Conditions;

– to satisfy contractual interests of Jobs Ops, if they do not conflict with the interests of the Data Subjects.

– for the satisfaction of the legitimate interests of the company or for the compliance with the regulatory requirements of the Labour Code, Ordinance No. 4 on the Documents Required for Concluding Employment Contract /, the Social Security Code, the Tax and Social Insurance Procedure Code, the Personal Income Tax Act, the Accountancy Act, the Obligations and Contracts Act, the Commerce Act, the Health and Safety at Work Act (HSWA), etc.

Aim of the policy

Jobs Ops legally processes the personal data of the Data Subjects for identification purposes in order to provide information and advertising services to the Consumers and as an employer in relation to its employees, applying the necessary organizational and technical measures provided for in the PDPA, Ordinance No. 1 of January 30 2013 for the minimum level of technical and organizational measures and the permissible type of protection of personal data.
The purpose of Jobs Ops is:

– compliance with applicable personal data legislation and following the good practices identified;

– to inform individuals for the purposes of personal data processing, recipients or categories of recipients to whom the data may be disclosed, the compulsory or voluntary nature of the provision of data, and the consequences of refusal to provide them;

– to provide information on the rights of data subjects, in accordance with the requirements of the applicable legislation;

– to ensure that data are processed lawfully and in good faith.

Personal data protection policy:

– protects the rights of natural persons – job applicants, representatives of clients and partners, as well as retention of the personal data provided by them;

– ensures that personal data are collected for specific, well-defined and legal purposes and are not further processed in a way incompatible with those purposes;

– undertakes actions/activities for data update, erasure or rectification of data when found to be inaccurate/inappropriate for the purpose for which they are being processed;

– establishes the necessary technical and organizational measures to protect personal data from unauthorized processing, unauthorized access, modification, dissemination and any other forms of illegal personal data processing;

– for better data protection, Jobs Ops may use data encryption or pseudonimisation.

Personal data collection

Jobs Ops collects personal information and is a Controller as regards the following categories of persons:

– individuals – Job Seeker Users;

– individuals representatives of Job Provider Users;

– visitors to the Site who identify themselves in case of questions, appeals, complaints, etc.;

– representatives of Jobs Ops partners;

– Jobs Ops employees.

The following data types are collected:

– name, surname, e-mail, telephone number in the case of Job Seeker Users, as well as position/occupation of Job Provider Users or Partners;

– bank details for payment purposes;

– personal identification number/personal number of foreigner, address, health information required in relation to the compliance with the regulatory requirements for employment and social security during the employment relationship and the required retention period thereafter with the employees of Jobs Ops.

Job seekers have the opportunity to store CVs and other documents, providing education, qualifications, employment data, contact details, as well as gender, residence, citizenship, etc. data.

The information in these documents is applied when applying, and in this process Jobs Ops appears as Data Processor of the data of Job Providers (Controller)

The platform also stores log data for:

– registration as Users for account login;

– acceptance with the GC, Personal Data Protection Policy and Cookies Policy;

– application by Job seekers;

– logs related to technical security.

Data subjects may not provide in any form whatsoever special ("sensitive") personal data – disclosing racial or ethnic origin, political views, religious or philosophical beliefs or trade union membership, genetic data, biometric data, health data status or data about sexual life or sexual orientation.

Data subjects – Users are not required to provide a PIN or PNF, either on registration or in the documents they store on the platform.

The Data Subjects – Jobs Ops employees provide PIN/PNF in the formation of employment and legal relations.

Retention periods

Jobs Ops stores and processes data for the purposes for which it was collected in accordance with the GC, the Personal Data Protection Policy and applicable law.

Personal data is stored by Jobs Ops until:

– withdrawal of consent of persons;

– the files required for application – until the withdrawal of consent or termination of registration;

– the acts defining the obligation to provide information to the court, competent state bodies, etc. the grounds provided for in the applicable legislation. Personal data erasure is not possible if it is necessary for legal or administrative proceedings to process a complaint of the data subject;

– logs related to electronic declarations of intent – 1 year;

– logs for logging in, system logs – 1 year.

– activity of the user account at least once every three years. After this period Jobs Ops has the right to erase all User data.

– payroll – 50 years;

– accounting records and financial statements – 10 years.

Rights of data subjects

1. Right of access to information – provides the data subjects with information about the categories of personal data being processed, the purpose of processing, the recipients to whom the data will be disclosed, the period within which they will be stored/processed, the right to rectify, erase or limit the personal data processing or to object to such processing, the right to human intervention in automated decision-making, the right to appeal to a supervisory authority.
2. Right of rectification – data subjects may request their personal data to be rectified in the event of inaccuracy or updating.
3. Right to data portability – the data subject is entitled to receive the data that he or she has provided to Jobs Ops in a structured, widely used and machine-readable format.
4. Right to erasure ("to be forgotten") – Jobs Ops is obliged to erase personal data on the following grounds:

- the data subject withdraws his/her consent;
- personal data are not necessary for the purposes for which they were collected;
- the data subject objects to the processing and there are no legal contradictory grounds thereof;
- personal data were processed illegally;
- personal data must be erased with a legal obligation on Jobs Ops.

Jobs Ops may fail to do so on any of the following grounds:
– for compliance with a legal obligation by Jobs Ops;
– in accordance with Article 9.2, h, and Article 9.3 of GDPR relating to interests in the field of public health.
5. Right to request restriction of processing – the data subject is entitled to claim restriction of the right of processing in:

– contesting the accuracy of personal data;

- improper processing, such as changing the purpose of processing

– the data subject has challenged the legitimate grounds of Jobs Ops until it is proved the personal interest shall prevail over the interest of Jobs Ops.

6. Right to object against the personal data processing – data may object against processing based on the legitimate interest of Jobs Ops, including for the purposes of direct marketing.
7. The right of the data subject not to be the subject of a decision based solely on automated processing which gives rise to legal consequences for the data subject, unless the grounds for the protection of personal data provided for in the applicable legislation exist.
Jobs Ops shall not make automatically data decisions.
8. Right to complain to a Supervisory Authority – if they consider that their rights have been violated, data subjects may file a complaint with the Commission for Personal Data Protection (CPDP):
Sofia 1592, 2, Prof. Tsvetan Lazarov blvd.
Email: kzld@government.bg, kzld@cpdp.bg
Phone: 02 9153518

Web: www.cpdp.bg

Categories of persons who access and process your personal data

1. Jobs Ops employees.
2. Job Provider employees.
3. Personal Data Processors/Partners.
4. Competent authorities having the power to request information from Jobs Ops, including personal data, e.g. – Bulgarian court, CPDP, Court of another state, etc.

Partners, subcontractors

In order to ensure the operation of the Site, its continuity, functionality, maintenance and functioning of Jobs Ops and as an organization, it is carried out in cooperation with Partners/Subcontractors. The employees of these companies may not retrieve, use, distribute or make available for use by other persons, erase or destroy data and other activities if they have access to a database containing personal data or other commercial/banking information in the course of their activities that are not relevant to their obligations.

DIGITAL OCEAN LLC, VAT ID: EU528002224, New York, NY 10013,101 Avenue of the Americas, 10th Floor – https://www.digitalocean.com/

Exercising of rights of data subjects

Requests for the exercise of rights may take any form that contains an unambiguous statement to that effect and identifies you as the data holder.

Email: dp@jobsops.com

Postal address and headquarters of Jobs Ops: Sofia 1000, 21 Lavele str,floor 5,tel.+359892040302

Technical and organizational measures for data protection

To ensure effective data protection, Jobs Ops applies all necessary organizational and technical measures provided for in the Personal Data Protection Act, Ordinance No. 1 of 30 January 2013 on the minimum level of technical and organizational measures and the permissible type of personal data protection, the guidelines and instructions of the Working Group under Art. 29, as well as CPDP and the GDPR Guidelines. The servers where the site is hosted are located in tightly secured data centres with adequate physical security and video surveillance.

The use of resources of https://jobsops.com/ by Users and Visitors is performed with 256-bit connection encryption.

The workstations that access the administration site are protected by 8-character passwords with the required level of complexity (letters, numbers, and symbols).

Jobs Ops employees may not copy personal data and other commercial/banking information of Users on external devices. If necessary, a protocol on the circumstances and purpose of this action should be established, applying additional safeguards such as encryption or pseudonymisation.

In order to prevent the destruction of some or all of the personal data, minimizing the damage in the event of a technical failure, viruses and hacking and continuous operation of the site, a minimum of one copy (Backup) of the database shall be made on a seven-day basis.

A data breach occurs when personal data is affected by an incident that violates the confidentiality, availability or integrity of personal data:

- accidental/unlawful destruction/loss, alteration, unauthorized disclosure of data by transmission;

– disclosure/destruction/modification of data as a result of an error or action by an employee or user;

– disclosure of data resulting from a hacking;

- in the case of unauthorized access to the personal data of an unauthorized employee or outsider;

- in case of incorrect processing, storage, disclosure of personal data by a partner/subcontractor of Jobs Ops.

In the event of a data security breach situation, all measures shall be taken immediately to prevent a continued breach, incl. also suspending access to the site of all Users/Visitors. The CPDP and the data subjects affected by the incident shall be notified within 72 hours.

Jobs Ops reserves the right not to notify data subjects if the information is encrypted/pseudonymized.

Recommended measures to Users:

– the access password must have the necessary level of complexity and may not be disclosed to third parties;

– when using a shared/assigned/publicly accessible computer, do not save your login information to the Site and always log out of your account after use;

– the responsibility for protecting your account information and any action taken from it is primarily your responsibility.

Amendments and Supplements to the Policy

Changes to our practices and the content of the Policy may be required at any time, and any updates made will be effective as from the date of publication on the Site, unless other period is published.