SPARTA CONSULTING

Sparta Consulting

Privacy Notice for Recruits and Job Applicants

Date: 17.1.2019
Version: 1.12

Contents

Purpose and scope of this privacy notice

The purpose of this Privacy Notice is to inform the job applicants of how Sparta Consulting Oy (later “we” or “Sparta”) processes personal data e.g. how personal data is collected, used and removed, and to whom the data is disclosed.

This Privacy Notice applies to the activities related to Sparta’s recruitment of new employees. The Privacy Notice concerns the job applicants (later “data subjects” or “you”) whose personal data Sparta processes related to the recruitment. When the job applicant uses Sparta’s products and services including web pages, the processing of personal data is described in the general Privacy Notice found on Sparta’s web pages. If the job applicant is hired, the processing of personal data continues according to the Privacy Notice for employees that will be submitted to the new employee.

The job applicants are strongly recommended to read this Privacy Notice before submitting any personal information related to a recruitment.

Sparta is committed to respect the job applicant’s privacy and processes the personal data related to the recruitment according to applicable privacy laws and regulations (especially the European Union’s General Data Protection Regulation (2016/679) and the Act on the Protection of Privacy in Working Life (759/2004)).

Personal data refers to information which allows a person to be directly or indirectly identified as an individual natural person (later “personal data”). Examples of personal data are name, address, date of birth and Internet Protocol (IP) address of a personal computer (PC).

This Privacy Notice uses the privacy terms defined in the in Article 4 of European Union’s General Data Protection Regulation (2016/679) (“GDPR”).

Data controller contact information

Sparta Consulting Oy
Business ID: 2507061-1
Address: Annankatu 22 c 14, 00100 Helsinki, Finland

Data Protection Contact: Harri Leinonen
Email: privacy@spartaconsulting.fi

Purpose and legal bases for the processing of personal data

We process the personal data of job applicants for recruitment purposes.

Purpose of processing of personal data	Legal basis for processing personal data
▸ Identifying job applicants for positions/roles (current and future) by searching for job applicants or obtaining/receiving job applications ▸ Communications (e.g. emails and phone calls) ▸ Evaluating and selecting job applicants for positions	Legitimate interests of Sparta for recruiting new employees and the job applicant's consent where necessary (see separate chapter below) If the job applicant is selected for a position/role, the legal basis includes the employment contract and its preparation, and the processing is continued according to the Privacy Notice for employees.
▸ Background checks: contacting references, credit check (as permitted by applicable law) and security screening (as permitted by applicable law)	Legitimate interest to ensure the security and safety of Sparta's business and Sparta's customers, suppliers, partners and other stakeholders. Consent: Background check processes are regulated by law and the consent of the job applicant is asked for whenever required.
▸ Storing the job applicant's application and related data for other recruitments than the one the job applicant has applied to or participated in ▸ Storing the job applicant's application and related data longer than described in this Privacy Notice for job applicants	Consent (The job applicant can withdraw his/her consent to any further processing of his/her personal data at any time by contacting the Controller, see contact information in the beginning.)
▸ Security and safety obligations (such as fraud prevention, access control and emergency response)	Legal obligations related to security and safety and legitimate interest to secure property
▸ Performing and administrating the exercise of rights under GDPR (see separate section on the rights of the data subjects / job applicants) and demonstrating compliance with laws and regulations	Legal obligation (data privacy legislation)
▸ Protection of legal rights e.g. to be able to defend a claim	Legitimate interest to protect Sparta's legal rights or legal obligation to protect someone else's rights

The personal data processed, sources and retention times

Sources of personal data

- The job applicant is the main source of personal data. He/she provides personal data by participating in a recruitment process managed by Sparta (e.g. submission of a job application, interviews, tests, communications)
- Sparta receives personal data of the job applicants from service providers (processors) that are utilised in evaluating and testing job applicants
- Sparta utilises third party recruitment services and publicly accessible sources to identify suitable job applicants such as LinkedIn.
- Sparta also receives personal data of the job applicants from others with the consent of the job applicant such as the current employees, the references submitted by the job applicant and the security screening agency

We only collect/obtain personal data relevant to the recruitment process. We collect the following categories of data:

Categories of personal data	Examples of personal data
Contact information	name, address, phone numbers, email address
Identity information	personal identification code or similar national identifier, date of birth, gender
Images	photo
Professional and education data	CV, education and training, employment history, employment details and work experience, employers, job titles, organizations, publications, professional skills, certificates
Other personal data submitted by the job applicant	other personal data than the afore mentioned and submitted by the job applicant on request or on his/her own initiative
Personality and suitability	aptitude and similar test results
Evaluation data	assessments of the job applicant's suitability for a current or future position in Sparta
Background check results	credit check and security screening results and answers/comments from contacted references

Job applicants are not obliged to provide personal data to Sparta but failing to provide information may result in termination of the individual recruitment process, or difficulties to evaluate the job applicant properly.

Retention periods

Sparta retains the job applicant's personal data as long as necessary for the purposes presented in this Privacy Notice, unless a longer retention time is required in the legislation.

If the job applicant is hired, the personal data processed in the recruitment process will no longer be pro-cessed under this Privacy Notice, it will be processed according to the employee privacy notice and the retention periods outlined there.

When the personal data are no longer needed, the data are removed or rendered anonymous within a rea-sonable time. The length of the retention period depends on the purposes of the processing. Retention times are presented in the table below.

Categories of personal data	Retention time
All recruitment data of a job applicant that has joined a recruitment process for a *specific position*(s)	24 months after the termination of the recruitment period (last update) unless the job applicant is hired where after the retention time is determined by the employee privacy notice NOTE! The security screening results are stored only 6 months as a maximum.
All recruitment data of a job applicant that has joined the recruitment process with an *open application*	24 months after the submission of the application unless the job applicant joins a recruitment process for a specific position, see retention times above
All recruitment data of a *potential* job applicant for a specific position	A potential job applicant is contacted within one month from obtaining the personal data or the data are removed. If the contacted job applicant agrees to join the recruitment process for a specific position or future positions (open application), see retention times above (Personal data of job applicants that have joined a recruitment process for a specific position(s)). If the job applicant rejects the offer to join the recruitment process, only necessary contact information is stored to be able to avoid contacting the same job applicant during the recruitment process for the same position. The data is removed when the recruitment process for the position is terminated, or at latest 6 months after the job applicant has been contacted. NOTE! The job applicant has the right to request all personal data to be removed at any time but will then take the risk of being contacted regarding the same position.

Data transfers and recipients

Sparta may transfer personal data of the job applicants to a recruitment service provider (independent controller) if the job applicant is personally evaluated by the recruitment company.

Sparta may perform background checks by transferring personal data to a credit data provider or the Finnish security intelligence service (Suojelupoliisi, SUPO) if permitted by applicable law, and with the consent of the job applicant if necessary.

In addition, Sparta's IT service providers may access the personal data processed by Sparta's IT systems (e.g. data storages) and equipment (e.g. computers) if necessary for performing the contracted IT services.

Recipients of personal data:

- Recruitment companies
- Credit information provider
- Security screening agency, Suojelupoliisi - SUPO (Finnish Security Intelligence Agency)
- IT service providers

More detailed information can be obtained from Sparta upon request.

Sparta may also disclose personal data due to a legal obligation related to e.g. security, safety and protection of legal rights.

If Sparta Consulting is involved in a merger, sale, joint venture, acquisition or similar arrangement, Sparta Consulting may transfer personal data to the parties involved. Sparta Consulting communicates any significant changes in the privacy to the job applicants whose personal data is concerned.

Personal data transfer(s) outside EU/EEA

Personal data of the job applicants is not transferred outside EU/EEA.

Rights of the data subject / job applicant

You have the rights stated in the GDPR to make the requests presented here.

- Right to access and rectification: You have the right to request us to inform you what personal data we process concerning you (or that no data is processed), and request us to correct your personal data that are incorrect or incomplete (or outdated)
- Right to erasure ('right to be forgotten') and right to restriction of processing: You have the right to request us to erase (or render anonymous) or restrict the processing of personal data concerning you that we process
    - We will comply with your request unless we have a legitimate ground not to delete the data, in which case you will be informed (After we have deleted your personal data, all backups might not be deleted immediately, but as soon as reasonably possible)
- Right to object to processing: You have the to object to the use of all or some of your personal da-ta for selected purposes
    - We will comply with your request unless we have a legitimate ground to continue the pro-cessing (e.g. legal obligation), in which case you will be informed
- Right to data portability: You have the right to receive the personal data concerning you that you have provided in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller (if the processing is based on consent or on a contract, and the processing is carried out by automated means)
- Right to withdraw consent: If you have given your consent to certain processing, you have the right to withdraw your consent at any time regarding further processing of your personal data
- Right to lodge a complaint to the supervisory authority: You have the right to complain to the com-petent supervisory authority if you believe your personal data has been processed incorrectly, but please contact us first to solve the issue with us, thank you!

We may request additional information if necessary to confirm your identity or clarify your request.

How to use these rights

You can use these rights by contacting us using the contact information found in the beginning of this Privacy Notice. The requests must be submitted in writing, and we need to confirm your identity, so we can make sure that we only disclose personal data to the person authorized to access the data. We may request additional information if necessary.

We will inform the recipients of your personal data if you have requested the data to be rectified, erased or restricted, unless this proves impossible (or involves disproportionate effort).

Where requests from a data subject are obviously unjustified or excessive, in particular because of their repetitive character, we may either:

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- refuse to act on the request.

Security measures

Sparta processes personal data in accordance with applicable data protection laws and regulations and ensure the compliance of the service providers (processors) with contractual measures (data processing agreements).

We have implemented modern technical and organizational security measures to protect personal data from unauthorised access or transfer and accidental or illegal destruction, loss or alteration. The information security and data protection of our systems and environments that contain personal data are managed appropriately as a whole. We ensure the security of the stored data, access rights and processing of the confidential and sensitive personal data.

Access to personal data is limited to those that need it for performing their work. Access is based on roles and the tasks and functions connected to that role. All persons processing personal data are required to treat the data as confidential. The users of the IT environment are identified and access to the systems is secured and limited by user rights. Access to the physical location is also based on individual access rights and access keys.

Version history and changes to this privacy notice

Sparta will update this privacy notice whenever necessary due to e.g. changes in our processes or recipients, or in the applicable legislation. We will publish the changes on our website and document them in the version history below. Significant changes may be communicated directly to those persons whose personal data is affected (and whose contact data is available).

Version history:

Version	Change	Date
1.1 First version published on the web page	Chapter 3: Clarification of the legal basis added. Chapter 6: The recruitment companies' role was changed from processor to independent controller. Clarification on the transfers added.	20.8.2018
1.2	Updated contact details and visual outlook	17.1.2019
1.3	Updated contact details and retention time for all recruitment data to 24 months	11.08.2021