Updated on 19 February 2024

KPO Cooperative Society Group's Job Applicant Register's

PRIVACY POLICY STATEMENT (as of 25 May 2018)

General Data Protection Regulation (EU) 2016/679, Articles 12, 13, 14 and 19

1. Controller

KPO Cooperative Society

Phone:	+358 20 780 7000
Postal address:	P.O. Box 516, 67101 Kokkola
Street address:	Prismantie 1, 67700 Kokkola
Business ID:	0242821-1

SOK Corporation is the data controller of the information in the job seeker profile.

2. Contact details of the data protection officer

tietosuojavastaava@sok.fi

3. Officer in charge of register matters

tietosuoja.kpo@sok.fi

4. Name of the register

KPO Cooperative Society Group's job applicant register

5. Purpose of processing personal data

Managing the job application process for the selection of suitable persons for vacant positions within the KPO Cooperative Society Group

6. Grounds for the processing of personal data

Executing a contract or the measures preceding execution. Consent, as applicable.

7. Description of the data controller's legitimate interest

The processing of personal data is not based on the data controller's legitimate interest.

8. Processed personal data and personal data groups

In the job advertisement: the name and contact details of the recruiting supervisor if they have been specifically included in the advertisement. Not included by default.

In the job application: Required: name, email address, phone number, language skills (if this information has been requested), whether the applicant has previously worked at S Group, and how they learned about us.

Voluntary: address, job-specific questions, link to a profile (e.g. on LinkedIn), degree information, work history.

The job applicant may also include their own CV information or other attachments.

The applicant may choose to create an applicant profile.

A video interview tool (RecRight) can be used in the recruitment process. When an applicant enters the RecRight service, the tool records the applicant's name, phone number, email address and a video that will be stored in RecRight's database. This information will also be collected from the supervisor who is responsible for recruitment and who has recorded the interview questions on video.

Aptitude evaluations carried out by an external partner may also be used in the recruitment process as necessary. In this case, the applicant's name, phone number and email address are provided to the partner.

With a job requiring special reliability, the applicant's credit information may be checked.

Open recruiting: In case the company has made open recruiting possible, then a person may fill in an open application.

Direct recruiting: The employer company may also seek employees through direct recruiting. In this case, a partner is used for the recruitment process, and the above information will be processed as applicable subject to the person's consent.

9. Groups of data subjects

Job seekers or the persons who are applying, or have applied, for a job in the data controller's service, or who have filled in the job application profile in order to later apply for a job in an S Group's company.

Contact information, background information, skills, work history

10. Data source and description of data sources if data is collected from public sources

The information in the register is mainly gathered from the job seeker. If any information is obtained from other sources than the job seeker, the job seeker's consent is separately requested for this (such as an aptitude evaluation by a partner) or the job seeker is separately notified of this (such as a credit information check).

11. Recipients of personal data

As a rule, personal data is not handed over. However, if the job seeker gives permission for this, their name, phone number and email address may be handed over to a partner for the purpose of an aptitude evaluation. Information may also be handed over to partners outside the S Group that process applications. After a person has been employed by the data controller, the personal data and contact

details they reported in their job application can be transferred to the employee register to grant access rights to S Group’s data systems and to identify the user.

When the video interview tool is used in the recruitment process, the applicant's name, phone number and email address as well as the recorded video will be transferred to the data controller's external partner. The same information concerning the supervisor responsible for the recruitment will also be transferred. RecRight will act as the processor of personal data.

We use a Google Analytics cookie to monitor visitors and measure the effectiveness of recruitment marketing.

12. Transfer of personal data to third countries or international organisations and data protection safeguards used

Personal data is not transferred outside the EU or the EEA.

13. Period for storing personal data or criteria for determining the storage period

Job application data is preserved for 2.5 years after the recruitment in question is closed, after which the data is erased.

The storage times are based on the limitation periods for bringing proceedings defined in the acts on equality and parity and limitation period for work discrimination offence under the Criminal Code.

14. Rights of the data subject

The data subject has the right to access their own personal data as laid down in Article 15 of the General Data Protection Regulation (GDPR).

The data subject has the right to demand that the data controller corrects eventual incorrect information as laid down in Article 16 of the Data Protection Regulation.

The data subject has the right to have their personal data removed in case the preconditions stated in Article 17 of the Data Protection Regulation are met.

The data subject has the right to restrict the processing of their personal data in case the preconditions stated in Article 18 of the Data Protection Regulation are met.

The data subject has the right according to Article 20 of the Data Protection Regulation to move the personal data from one system to another for the part for which the data was received from the data subject, its processing is automatic and its processing is based on consent or agreement. The data subject has the right, based on Article 21 of the Data Protection Regulation, to object to the processing of the data that applies to them, in case the data was gathered in order to perform a task that concerns the common good, or based on legitimate interest, in case the other criteria included in the Article are met.

If a data subject wishes to exercise their rights or to obtain further information on the processing of their personal data, they may contact the controller named in this privacy policy. You can find more information on rights on the Your Rights page.

The data subject has the right to file a complaint with the supervisory authority.

15. Withdrawing consent

So far as the processing of the information is based on consent, the data subject has, according to Article 7 of the Data Protection Regulation, the right to withdraw their consent at any time. After the withdrawal, the data controller no longer has the right to use the personal data for such purposes that have no other grounds for processing except for the consent. Consent may be withdrawn by notifying it to the data controller.

16. Effects of not providing personal data on an agreement

In case a job seeker does not provide their personal data that the data controller needs, it is possible that he/she cannot be selected for the applied task.

17. Significant information related to automated decision-making or profiling

No automated decision-making or profiling is associated with the personal data processing.

18. Impact of the processing of personal data and a general description of technical and organisational security measures

Processing the data complies with the legislation pertaining to processing, protecting and disclosing the data of private persons as well as the information security guidelines of SOK Corporation and the regional cooperatives.

Based on the log files, it is possible to investigate possible misuse and alterations in the register.

Access rights to the register are clearly defined and restricted to those persons whose work tasks include taking care of recruitment.

We diligently protect personal data throughout its lifecycle by employing the appropriate data protection and information security measures. System providers process personal data at secure server facilities. Access to personal data is restricted and our personnel is subject to a non-disclosure obligation.

At S Group, we protect personal data with, among other things, anticipatory risk management and security planning, data communication protection means, the continuous maintenance of information systems and backups and by using secure hardware facilities, access control and security systems. After initial processing, the physical documents that contain personal data are kept in locked and fireproof storage areas. The granting and monitoring of user rights is a well-managed process. We regularly provide training for our personnel who participate in the processing of personal data, and ensure that our partners' personnel also understand the confidential nature of personal data and the importance of secure

processing. We select our subcontractors with care. We continuously update our internal practices and guidelines.

If, despite all our protective measures, personal data falls into the wrong hands, there is a possibility that this data will be misused. If we notice that such an event has happened, we will immediately begin an investigation and will make efforts to prevent any damage from occurring as a result. We will inform the relevant authorities and data subjects of any information security breaches in accordance with legislative requirements.