

Applicant Register**PRIVACY NOTICE (effective as of 25 May 2018)****General Data Protection Regulation of the European Union (EU) 2016/679, Articles 12, 13, 14 and 19**

| | |
|--|--|
| 1. Controller | For the data in the applicant profile, the controller is Suomen Osuuskauppojen Keskuskunta (SOK). For recruitment data (the application form and its attachments), the controller is the S Group company to which the applicant applies for a job. |
| 2. Contact details of the Data Protection Office | Mikko Viemerö, tietosuojavastaava@sok.fi |
| 3. Person responsible for register matters | <u>At SOK:</u> Tapio Syrén, tapio.syren@sok.fi In regional cooperatives and subsidiaries, register matters are handled by the HR unit of each employer company. Further information and contact details: |
| Etelä-Karjalan Osuuskauppa | tietosuja.eekoo@sok.fi |
| Etelä-Pohjanmaan Osuuskauppa | eepee.tietosuja@sok.fi |
| Helsingin Osuuskauppa Elanto | hok-elanto.tietosuja@sok.fi |
| Inex Partners Oy | tietosuja.inex@sok.fi |
| Jollas-Opisto Oy | tyosuhdejuristit@sok.fi |
| Kauppakeskus Mylly | tyosuhdejuristit@sok.fi |
| Koillismaan Osuuskauppa | koillismaa.tietosuja@sok.fi |
| Kymen Seudun Osuuskauppa | kso.tietosuja@sok.fi |
| Meira Nova Oy | tietosuja.meiranova@sok.fi |
| Osuuskauppa Arina | arina.tietosuja@sok.fi |
| Osuuskauppa Hämeenmaa, ml. Nelipyörä Oy | tietosuja.hameenmaa@sok.fi |
| Osuuskauppa Keskimaa | tietosuja.keskimaa@sok.fi |
| Osuuskauppa Keula | keula.tietosuja@sok.fi |
| Osuuskauppa KPO, ml. Automa Oy ja Oy Autoliike Nystedt Bilaffär Ab | tietosuja.kpo@sok.fi |
| Osuuskauppa Maakunta | tietosuja.maakunta@sok.fi |
| Osuuskauppa PeeÄssä | tietosuja.peeassa@sok.fi |
| Osuuskauppa Suur-Savo | tietosuja.suur-savo@sok.fi |
| Pirkanmaan Osuuskauppa | tietosuja.pirkanmaa@sok.fi |
| Pohjois-Karjalan Osuuskauppa | tietosuja.pko@sok.fi |
| Reila Palvelut Oy | info.reila@sok.fi |
| Satakunnan Osuuskauppa, ml. Palin Oy | tietosuja.satakunta@sok.fi |
| S-Business Oy | tyosuhdejuristit@sok.fi |
| S-Herkkukeittiö Oy | hok-elanto.tietosuja@sok.fi |

| | |
|---|---|
| SOK Liiketoiminta Oy | tyosuhdejuristit@sok.fi |
| Sokotel AS | tietosuoja.assokotel@sok.fi |
| Sokotel Oy | sokotel.tietosuoja@sok.fi |
| S-pankki-konserni, ml. FIM Oyj | tietosuoja@s-pankki.fi |
| Suomen Osuuskauppojen Keskuskunta (SOK) | tyosuhdejuristit@sok.fi |
| Suur-Seudun Osuuskauppa, ml. Lohjan Autokeskus Oy ja PP-Auto Oy | sso.tietosuoja@sok.fi |
| Turun Osuuskauppa | tok.tietosuoja@sok.fi |
| Varuboden-Osla Handelslag | vbo.tietosuoja@sok.fi |
| 4. Name of the register | Applicant Register |
| 5. Purpose of the processing of personal data | To manage the recruitment process when selecting individuals for positions that become vacant within the S Group. |
| 6. Legal basis for the processing of personal data | Legitimate interest Consent, where applicable (for example direct search and suitability assessments). |
| 7. Description of the controller's legitimate interest | <p>The controller has an interest in being able to select the most suitable employees for the positions, and without the processing of personal data the recruitment process would not be possible. The processing does not cause harm to the data subject; instead, it supports the applicant's own objective, i.e. obtaining employment with the controller. The controller has a significant legal interest in retaining personal data after the recruitment decision has been made, and this also serves to safeguard the data subject's legal protection.</p> <p>In certain situations, the controller has an interest in contacting persons who have previously been employed by the controller and inquiring about their willingness to enter into a new employment relationship. This processing does not cause harm to the data subject, but may enable a new employment relationship and efficient recruitment.</p> |
| 8. Categories of personal data processed | <p><u>In the job advertisement:</u> The name and contact details of the recruiting supervisor, if they have been specifically included in the advertisement. This is not the default.</p> <p><u>In the job application:</u> Mandatory: name, email address, phone number, language skills (where requested), whether you have previously worked for the S Group, and how you heard about us.</p> |

Voluntary: address, position-specific questions, link to a profile (e.g. LinkedIn), qualification details, employment history.

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

The applicant must create an applicant profile in the recruitment system. To create an applicant account, an email address and a password chosen by the applicant are required. The applicant can also choose to create the account using Google or Apple credentials, which means that Google/Apple will disclose the applicant's email address to the employer.

A video interview tool (RecRight) may be used in recruitment. In that case, the following are collected on transfer to the RecRight service: the applicant's name, phone number, email address and a video, which is stored in RecRight's own database. The same information is collected about the responsible recruiting manager who has recorded the interview questions on video.

Suitability assessments performed by an external partner may also be used in recruitment where necessary. In such cases, basic information about the applicant is provided to the partner, depending on the situation, for example the applicant's name and contact details and information on the position applied for. In the suitability assessments, applicants provide answers to assessment tasks, and an assessment report is produced on the basis of these answers.

With the applicant's consent, references about the applicant may also be collected.

For positions requiring particular reliability, the applicant's credit information may be checked.

Open recruitment: If the company has enabled open applications, a person may submit an open application.

At the end of the recruitment process, applicants may be sent a link to an applicant survey; responding is voluntary.

Direct search: The employer may also search for candidates by means of direct search. Direct search is carried out both by SOK's recruiters and with the assistance of partners. In direct search, the above-mentioned data are processed, where applicable, with the person's own consent.

| | |
|---|--|
| | <p>The employer may contact former employees to ask whether they would be interested in a new employment relationship. For this purpose, the former employee's contact details, i.e. phone number and/or email address, are used. After such an enquiry, any recruitment and/or hiring process continues in accordance with the normal process.</p> |
| <p>9. Categories of data subjects and categories of personal data</p> | <p>Job applicants, i.e. persons who are applying or have applied for a job with the controller, or who have completed an applicant profile in order to apply later for a position in an S Group company.</p> <p>Contact details, background information, information on skills and competencies, employment history, answers given by the applicant during the recruitment process (interviews, video interviews, suitability assessments) and the assessments generated on the basis of these.</p> |
| <p>10. Source of data and description of data sources if data have been collected from public sources</p> | <p>The data in the register have primarily been obtained from the job applicant themselves. If data are collected from a source other than the applicant, the applicant's consent will be separately requested (for example for a suitability assessment by a partner) or the applicant will be separately informed (e.g. credit information checks). The applicant can choose to use Google or Apple credentials to create an applicant account, which means that Google/Apple will disclose the applicant's email address to the employer.</p> |
| <p>11. Recipients of personal data</p> | <p>As a rule, personal data are not disclosed. However, the basic information of the person (see section 8) may be disclosed to a partner for the purpose of conducting a suitability assessment, with the applicant's consent. Data may also be disclosed to contractual partners outside the S Group who process applications.</p> <p>When a person is selected for employment with the controller, the phone number provided in the job application may be transferred to the employee register for the purposes of granting access rights to S Group information systems and identifying the user.</p> <p>Where a video interview tool is used in recruitment, the applicant's name, phone number, email address and recorded video are transferred to the controller's external contractual partner (RecRight). The same data are transferred concerning the responsible recruiting manager. RecRight acts as a processor of personal data.</p> |

| | |
|---|--|
| | |
| 12. Transfer of personal data to third countries or international organisations and safeguards used | Personal data are not transferred outside the EU/EEA. |
| 13. Retention period of personal data or criteria used to determine the retention period | <p>Data on job applicants are retained for 2.5 years from the closing of the relevant recruitment process, after which the data are deleted.</p> <p>Retention periods are based on the limitation periods under equality, criminal and non-discrimination legislation.</p> |
| 14. Rights of the data subject | <p>The data subject has the right to access their personal data in accordance with Article 15 of the GDPR.</p> <p>The data subject has the right to request that the controller rectify any inaccurate data in accordance with Article 16.</p> <p>The data subject has the right to have their data erased where the conditions in Article 17 are met.</p> <p>The data subject has the right to restriction of processing where the conditions in Article 18 are met.</p> <p>The data subject has the right to data portability under Article 20, insofar as the data have been provided by the data subject, are processed by automated means and the processing is based on consent or a contract.</p> <p>The data subject has the right to object to the processing of their personal data under Article 21, where the data have been collected for the performance of a task carried out in the public interest or on the basis of legitimate interest, and the other conditions in that Article are met.</p> <p>If a person wishes to exercise their rights or obtain further information about the processing of their personal data, they may contact the controller specified in this notice.</p> <p>The data subject has the right to lodge a complaint with the supervisory authority.</p> |
| 15. Withdrawal of consent | <p>Insofar as the processing of data is based on consent, the data subject has the right under Article 7 of the GDPR to withdraw their consent at any time.</p> <p>Withdrawal of consent ends the controller's right to process personal data for those purposes which do not have any other legal basis besides consent. If consent is withdrawn after the selection decision has been made, the controller has the right and interest,</p> |

| | |
|--|---|
| | <p>in order to defend against legal claims, to retain the data until the end of the defined retention period. Consent can be withdrawn by notifying the controller. Insofar as the processing of data is based on consent, the data subject has the right under Article 7 of the GDPR to withdraw their consent at any time. Withdrawal of consent ends the controller's right to process personal data for those purposes which do not have any other legal basis besides consent. If consent is withdrawn after the selection decision has been made, the controller has the right and interest, in order to defend against legal claims, to retain the data until the end of the defined retention period. Consent can be withdrawn by notifying the controller.</p> |
| 16. Consequences of failure to provide personal data for the contract | <p>If the job applicant does not provide the personal data required by the controller, it may not be possible to select them for the position applied for.</p> |
| 17. Meaningful information about automated decision-making or profiling | <p>The processing of personal data does not involve automated decision-making, nor is profiling carried out on the basis of personal data.</p> |
| 18. Effects of the processing of personal data and general description of technical and organisational security measures | <p>In the processing of data, legislation concerning the processing, protection and disclosure of personal data is complied with, as well as the data security guidelines of the SOK Group and the regional cooperatives.</p> <p>With the help of log files, it is possible to investigate, among other things, misuse and changes made to the register.</p> <p>Access rights to the register are carefully defined and limited only to those persons whose duties include handling recruitment.</p> <p>We carefully protect personal data throughout their lifecycle by using appropriate data protection and data security measures. System providers process personal data in secure server facilities. Access to personal data is restricted and staff are bound by a duty of confidentiality.</p> <p>Within the S Group, we protect personal data, among other things, through proactive risk management and security planning, protection of data communications, continuous maintenance of information systems, back-up procedures and by using secure equipment facilities, access control and security systems. Physical documents containing personal data are stored, after initial processing, in locked and fireproof storage facilities. Granting and monitoring of access rights is controlled. We regularly train staff involved in the</p> |

processing of personal data and ensure that the staff of our partners also understand the confidential nature of personal data and the importance of secure processing. We carefully select the subcontractors we use. We continuously update our internal practices and guidelines.

If, despite all our protective measures, personal data end up in the wrong hands, there is a risk that identity theft or other misuse of personal data may occur. If we detect such an incident, we immediately start investigating and aim to prevent or minimise any harm caused. We inform the relevant authorities and the data subjects about a data breach in accordance with legal requirements.

We use the Google Analytics cookie for visitor tracking and for measuring the effectiveness of recruitment marketing.