

COMMUNICATION AND MARKETING PRIVACY NOTICE

Summary

This summary explains how StaffPoint processes the personal data of individuals included in its communications target groups. Detailed information about processing activities can be found in the communications and marketing register privacy notice below.

On what basis do we process your personal data?

At StaffPoint, the processing of your personal data is based on your consent, a contract between us, or StaffPoint's legitimate interest. You may have a customer or employment relationship with us, have applied for a job through us, or contacted StaffPoint via communication channels and expressed potential interest in us. You may also be a contact person for a potential customer of StaffPoint, a subscriber to our newsletter, or have otherwise given us marketing permission in some context.

What data do we collect about you?

We only collect information about you that is necessary for communication between StaffPoint and you in connection with our company. Such information includes, for example, your email address, name, position in your company, and your social media address. We do not process your data for any purposes other than these.

Where do we obtain your data?

As a rule, the personal data we store has been obtained from you: from a request for quotation or other expression of interest in our services, from a contact form you have submitted, a job application, or your response to our campaign. You may have subscribed to our newsletter or given your consent for data processing at some event.

Personal data may also be collected from public sources or from companies providing personal data services.

We process your data only for as long as necessary, after which we delete the data from our register.

To whom do we disclose your data?

We disclose your data only to the providers of our communications and marketing tools, solely for the purpose of delivering the service. All parties to whom your data may be disclosed for justified reasons have entered into legally required data processing agreements, and your data is always handled confidentially.

How do we protect your data?

We use methods and systems for processing personal data that ensure your data is protected in the best possible way. Access to your data is restricted by user rights and appropriate technical security measures. All personnel involved in processing your data are bound by confidentiality obligations and take all necessary measures to protect your privacy.

StaffPoint Communications and Marketing Privacy notice

1. Controller

StaffPoint Group
Ruoholahdenkatu 14, 00180 Helsinki

2. Person Responsible for Data Protection

tietosuoja@staffpoint.fi

3. Purpose and Legal Basis for Processing Personal Data

The legal basis for processing personal data under the EU General Data Protection Regulation is:

- Performance of a contract: the individual's customer or employment relationship with StaffPoint Group
- The individual's consent (for example, contact via online service, phone, or email, or marketing consent given in a job application)
- StaffPoint's legitimate interest to offer its services to company contacts whose contact details are available from public sources or from companies providing personal data services.

The purpose of processing personal data is to inform about matters related to StaffPoint Group and to market services in the form of newsletters or targeted marketing campaigns. Personal data is not used for automated decision-making or profiling.

5. Groups of Data Subjects

Contacts of StaffPoint Group's customers and potential customers, StaffPoint employees and job applicants, and individuals who have electronically subscribed to marketing messages from StaffPoint.

6. Categories of Personal Data

The following data may be stored in the StaffPoint Group communications and marketing register:

- Name, position, company/organization, contact details (phone number, email address, address)
- Website addresses, IP address of the network connection, usernames/profiles in social media services
- Information about ordered services and their changes
- Data obtained from acceptance of cookie policies regarding visits to StaffPoint's websites and areas of interest

7. Recipients and Recipient Groups of Personal Data

- StaffPoint may disclose personal data as necessary between group companies.
- StaffPoint uses subcontractors who process personal data on its behalf. Subcontractors act as system and service providers for StaffPoint. Appropriate data processing agreements have been made with subcontractors, which include confidentiality obligations in addition to processing terms.

8. **Transfer of Data Outside the European Union or European Economic Area**

Personal data is primarily processed only within the EU/EEA. In certain cases, personal data may also be processed technically outside the EU/EEA. In such cases, StaffPoint ensures an adequate level of data protection as required by law.

9. **Retention Period of Personal Data**

Data is retained in the register for as long as necessary or until the data subject withdraws their consent for processing.

After withdrawal of consent or expiration of the retention period, the controller will properly destroy all data concerning the data subject, regardless of the storage format.

10. **Rights of the Data Subject and How to Exercise Them**

For all matters related to data protection and the processing of personal data, please contact StaffPoint Group's data protection at tietosuoja@staffpoint.fi.

If a data subject wishes to inspect their personal data or obtain other information about the processing of their data, they must prove their identity when making the request, either through strong electronic identification or by presenting an official identity document at a StaffPoint office.

- **Right of Access – Inspection Right**

Data subjects have the right to inspect the data concerning themselves in the register. To do so, the data subject must submit a written, personally signed or similarly verified request to the controller or present the request in person at the controller's premises. The data subject must also prove their identity when making the request. The controller will provide the requested data without undue delay:

- Electronically, if the data subject has requested this and if it is possible in a secure manner.
- Or arrange an opportunity to review the stored data at one of the controller's offices.

- **Right to Rectification, Erasure, and Restriction of Processing**

The data subject has the right to request the rectification or erasure of incorrect or inaccurate data in the register, or to restrict processing.

- **Right to Object to Processing**

The data subject has the right to object to the processing of their personal data.

- **Right to Data Portability**

The data subject has the right to request the transfer of data they have provided in a machine-readable format.

11. **Withdrawal of Consent**

The data subject has the right to withdraw their consent to the processing of their personal data at any time.

The data subject may withdraw their consent to receive communications and marketing messages by using the channel-specific opt-out function or by sending a request for data deletion to the controller.

After withdrawal of consent, the controller will no longer process the data subject's data for these purposes.

12. **Right to Lodge a Complaint with a Supervisory Authority**

If the data subject considers that the processing of personal data is unlawful, they have the right to lodge a complaint with the supervisory authority.

13. Sources of Data, Regular Sources of Data

Data stored in the register is obtained from our customer relationship management system (existing or potential customers who have contacted us) or from the individual, e.g., from messages sent via web forms, by email, by phone, through social media services, from events and occasions where the individual provides their data. In addition, personal data may also be collected from public sources or from companies providing personal data services.

14. Automated Decision-Making Including Profiling

Personal data is not used for automated decision-making or profiling.

15. Principles of Register Protection

Care is taken in the processing of the register, and data processed via information systems is appropriately protected. When register data is stored on internet servers, the physical and digital security of the hardware is properly ensured. The controller ensures that stored data, server access rights, and other information critical to the security of personal data are handled confidentially and only by employees whose job description includes such processing.