Privacy notice for recruitment

1 Purpose of this privacy notice

As an employer, Rosti ("we") aim to attract candidates and recruit employees for various positions worldwide, using direct recruitment, recruitment services and web solutions. We also target young talents by cooperating closely with educational institutions in all locations we have business units.

You are reading this privacy notice because you have either applied for an open position in Rosti or you have been suggested to Rosti as potential candidate.

During a recruitment process we will process personal information about you. This means that we are a "data controller" and that we are responsible for deciding how we hold and use personal information about you.

The purpose of this Privacy Notice is to make you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, with whom we might share it and how long it will usually be retained for. It provides you with certain information that must be provided under the General Data Protection Regulation (*(EU) 2016/679*) (GDPR).

We respect your privacy and will protect any of your personal data that we collect, use and store.

2 Why and what grounds we collect and use your data

The purpose for processing your personal data is to collect and review applications from job applicants and the ground for processing of your personal data is based on our legitimate interest to select a best fitting employee for the position and for the Rosti.

The recruitment process includes the following steps where your personal data will be used:

- collecting and registering applicants and the associated information
- pre-screening candidates
- interviewing
- testing and assessment of your skills, qualifications and suitability for the position
- references, background check if necessary
- decision making
- communication with you
- keeping records related to our hiring processes
- complying with legal or regulatory requirements

By providing us the required necessary information about you, your qualification and work history allows us to make fair and beneficial decision for both parties.

In case the recruitment is concluded with decision to offer you the job, the personal data collected during the recruitment process will be used to provide a job offer and the employment contract.

If you are hired, the relevant personal data collected during the recruitment process will be processed by us to fulfil the contractual obligation set forth in the employment agreement and to fulfil any mandatory obligations set forth by the applicable laws. How and why we process person data of our employees is set out in a separate privacy notice available on www.rosti.se/privacy.

In specific cases your data may be used for fulfilling our statutory obligation whether locally or a group level.

3 Personal information we collect about you

We collect and use personal information provided by you in your job application, CV, cover or motivation letter and/or related documents, or any subsequent information you have provided during the recruitment process.

In connection with recruitment we will collect and use the following categories of personal information about you (the extent provided and relevant):

- name, gender and birth date
- contact information – e-mail, home address, phone, Skype address etc.
- information of your qualification and education
- information of your work experiences, employment history and current position
- information relating to the evaluation your suitability for the position as well as personal qualities relevant in respect of the position
- information received from references you have named relating to your former performance and suitability as well as personal qualifications relevant for the position
- any information you have provided us during the interviews
- test results and assessment information relating to the position

If you are applying for a senior position or if required by mandatory applicable law, we may also collect and use the following "special categories" of more sensitive personal information necessary due to the nature, scope and/or security requirements related to the position in question:

- criminal records
- information about your health, may include any medical condition, health and sickness records

In case you provided personal information that is not necessary for the recruitment (e.g. marital and family or family members' details), we will not process this data or use it in recruitment process. Nevertheless, we will apply the same respect and security measures as for any personal data until it has been deletion.

Please be aware that you have a responsibility to ensure that any information you send is within the bounds of the law.

If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully.

4 Other sources we may use to get information about you

Additional necessary information regarding to your work history, qualification and suitability for the position may be obtained from:

- recruitment service providers or consultants providing recruitment services, e.g. pre-screening and interviewing applicants and handling candidates testing or assessments as a part of the recruitment process
- reference persons whose contact details you have provided to us
- social media designed for recruitment purposes, like LinkedIn
- in rare cases also from publicly-available websites.

Also, subject to the applicable laws and your consent, information may be obtained through background checks, security clearances and other similar information sources deemed necessary due to the nature and security requirements related to the open position in question.

5 Automated decision making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making. There will be always human intervention into automated analytics, e.g. testing of personality.

6 Sharing personal data

Sharing with service providers

Your personal data may be disclosed to recruitment service providers or consultants when Rosti requires such services. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Sharing within Rosti

As we are international company group, your personal data may be shared with other entities of Rosti group during international recruitments. International recruitment is either for higher managerial positions, international talent recruitment and/or there is requirement of "grandfather's" (manger's manager) approval.

All our third-party service providers and other entities in the Rosti group are required to take appropriate security measures to protect your personal data in line with our policies. We ensure the security obligation is in applied with data protection contracts.

In case our recruiting or involved entity is located outside of EU/EEA, we may transfer your personal data outside of EU/EEA during international recruitments. In such situations, we ensure that sufficient level of data protection is maintained through appropriate safety measures, and unless the transfer is made to a country deemed by the EU Commission to provide sufficient protection the transfer will be based upon the EU Commission's model clauses / standard contractual clauses.

We do not sell, hire out, distribute or otherwise make your personal data available to any third party other than what is set out above.

7 Data Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We limit access to your personal data to those employees, agents, contractors and other third parties who have "need to know", i.e. who need the access in order to fulfil the tasks and duties relating to the recruitment or role (e.g. HR). They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

Our IT systems are protected against unauthorized access with various data protection functions. When your personal data is collected or used in digital form, system or folders, each user has a personal user ID and password or defined access rights to access to your personal data. Our IT & DPO monitoring the safety and integrity of the IT environment and other communications channels on regular basis and have

implemented technical measures to prevent and detect any safety breaches that may threaten your personal data.

The integrity of personal data is also ensured when transferring or disclosing your personal data. The applied safety measures vary based on the sensitivity of the data and may include e.g. strong identification of the recipient and encryption of the transferred information.

Our recruitment and IT and communications service providers are required to be compliant and demonstrate the compliance with Personal Data Protection requirement, and we have sufficient data protection clauses or agreements with all service providers, including confidentiality obligations.

Any sensitive information (such as health-related information or any sensitive data required by local legislation) will be always used separately from other personal data and access rights to such sensitive personal data are granted only with substantial reasons to persons making decisions and have ultimate responsibility of quality of recruitment, usually HR representatives, direct manager and direct manager's manager.

We have implemented procedures to deal with any actual or suspected data security breach and will notify you and any applicable authority about breach where we are legally required to do so.

We are avoiding personal data collection and usage in paper format in recruitment process. If so, CVs and applications in paper will be always stored in secure premises and destroyed after recruitment has ended. In case contracting process follows the relevant documents demanded to be stored in paper format will be part of individual records and stored in locked premises. Such data will be used only by such employees of Rosti who have a justified reason for doing so as a part of his/her duties.

8 Data Retention

After the recruitment process has ended, we retain your personal data in identifiable format for no longer than twelve months based on our genuine needs (e.g. the chosen candidate declines the offer to join, and we decide to approach to another candidate) and legislative requirements (e.g. to satisfy any claims or questions raised by candidate). After twelve months either we will deleted your personal data and documents provided by you or anonymise for recruitment statistics purposes. However, in certain cases, e.g. for purposes of defending us against an actual or potential legal a claim, or if otherwise necessary in relation to legal proceedings or defending a legal right or if the local legislation requires for a longer retention period, certain information may be retained for longer.

In case our interest is to save your data into our "application bank" for future recruitments, the local Rosti site HR representative will contact you and requires your consent to do so with provision of relevant information. This is voluntary and you have right to decline such request. Our "application bank" is reviewed on regular bases and the maximum retention time for your data in our "application bank" is up to two years. However the tests and profiling done during the recruitment will be stored up to 6 months.

When an candidate is chosen for the position, his/her personal information relevant for the employment relationship shall be transferred to Rosti's employee register or system. When candidate is already employed by Rosti, the information relating to the fact that he/she applied for the position, may be retained even if the person is not selected for the position until the termination of employment relationship.

9 Your rights in connection with personal information

If you are an EU citizen or if your personal data in processed by a Rosti entity based in the EU and in accordance with the GDPR, you have the right to:

- **Request access to your personal information**. This enables you to receive a copy of the personal information we hold about you and to check that we are collecting and using it lawfully.
- **Request correction of the personal information that we hold about you**. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure of your personal information**. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to use it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing of your personal information** where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- **Request the restriction of collecting and using your personal information**. This enables you to ask us to suspend the usage of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer of your personal information** to another party.
- **Right to lodge a complaint** to supervisory authority.

When you make request, you must provide credentials with which it is possible to verify your identity, such as a copy of your passport, driver's license, EU ID-card, etc.

We are not using your personal data for direct marketing.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact with PDP responsible person of local Rosti site or Rosti DPO in writing.

10 Contact details

10.1 Data Controller, Employer

Name:	Rosti Group AB
Address:	Anna Lindhs Plats 4, Malmö
Contact details:	Tel: +46 4020 4709

10.2 Rosti DPO (Data Protection Officer)

Name:	Mari Lüdimois
Contact details:	e-mail: dpo@rosti.com
	phone: +48 7818 20 583

11 Contacting the Data Controller

In all questions and matters relating to personal data we are collecting and using or your rights as the data subject, you should contact either with local PDP Responsible person or with the DPO by dpo@rosti.com.

We are do not charge you for exercising your rights presented in Section 9. However, we have right at our sole discretion to refuse to fulfil or charge a reasonable fee for fulfilling of several similar consecutive requests or requests that are manifestly unfounded or excessive. We are also entitled to decline requests on statutory grounds in which cases we will inform you of such decline including the grounds for the decline.