Policy Owner
Data Protection Officer

Responsible officer
Data Protection Officer

Approved By
EMT, 2018-04-12

Valid from
2018-05-25

Version
1.0 2018-05-25

Group policy

Rosti Personal Data Policy

The Rosti Personal Data Policy (the "**Policy**") sets the framework and necessary conditions to ensure an adequate level of Personal Data Protection within our operations, and is the foundation of Rosti's Personal Data Protection program. All employees, board member or other representative of Rosti shall Process Personal Data in compliance with the Policy and applicable Data Protection Laws.

Introduction and objectives

All legal entities owned by Rosti Group AB, irrespective of the country of registration of such legal entity (jointly referred to as "**Rosti**") are committed to the highest norms of business conduct. As such, our business operations shall be based on our Code of Conduct, advocating fair competition and ethical conditions within the legal frameworks of the countries where we are located or otherwise operate.

Engaging in behaviour or activities contrary to applicable laws and regulations and/or Rosti's Code of Conduct, not only violate our promise to our stakeholders but may also result in negative effect on Rosti's good reputation as a fair and ethical business partner. It may also result in sanctions for both Rosti and the individuals involved.

Rosti shall consistently comply with all relevant laws and rules applicable in the markets in which Rosti conducts business, including but not limited to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (the "**General Data Protection Regulation**" or the "**GDPR**"). Additionally, we shall comply with the laws implementing or supplementing the GDPR and, to the extent applicable, the Data Protection Laws of any other country outside the European Union.

We have dedicated global resources and establish Compliance Governance Standard to ensure compliance with applicable Data Protection laws and we strive to embed Data Protection by default and design into our operations, and assist employees, board members and Business Partners.

Our customers or suppliers are never individuals and we do not target the end-consumer, therefore we Process information about natural person mainly in order to fulfil our contractual or legal obligations or on the basis of our legitimate interests.

Additional public information on Rosti Personal Data Processing is available on www.rosti.com/privacy or by contacting our Data Protection Officer on dpo@rosti.com.

For employees all information, the current version of the Policy, guidelines and tools are available in RostiNet/Rosti Data Protection sub-site. Additional information could

be acquired by contact with Data Protection Officer on dpo@rosti.com or with local nominated responsible persons.

Scope and deviations

The Policy serves as a minimum standard for Rosti Data Protection. The Policy does not override any applicable national Data Protection Law and regulations in countries where the Company operates.

The Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

As Rosti is a Swedish owned company group with operations, customers and suppliers both within Europe and outside, the Policy will apply to all Rosti entities, regardless of location. All entities within Rosti are bound to comply with our requirements which are further regulated by intra-group agreements.

The Policy applies to all employees and board members of every company within Rosti. It also applies to Rosti employees working in joint ventures and other comparable business partnerships and arrangements in which Rosti participates.

Rosti expects that all our Business Partners and any such Business Partners' sub-contractor applies provisions not less strict than what is set out in the Policy and in mandatory law.

Individual Rosti companies are not entitled to adopt regulations that deviate from the Policy. Additional data protection policies can be adopted in agreement with the Data Protection Officer only if applicable national laws require higher standards regarding Personal Data Protection.

If a local law prevents us from applying the Policy or prevents a Rosti entity to fulfil its obligations under the Policy and where complying with such local law would have an adverse effect, the matter shall be reported to the DPO and Rosti Personal Data Team as soon as possible.

Definitions

The following definitions apply in the Policy:

Personal Data means any information related to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This includes personal information regarding Rosti employees and Business Partner's contact persons.

Sensitive Personal Data means special categories Personal Data defined in the Regulation (racial or ethnic origin, political opinions, religious of philosophical beliefs, trade union membership, Processing of genetic or biometric data, data concerning

health, sex life or sexual orientation). Additional legal requirements apply to the Processing of Sensitive Personal Data, such as the requirement to ask a Consent form the Data Subject in certain situations, and the requirement for additional security measures.

Processing (Process) means any operation or set of operations performed upon Personal Data, regardless of methodology. This includes collecting, storage, alteration, retrieval, use, disclosure, making available, erasure, destruction etc.

Data Protection Laws means any applicable Personal Data protection or privacy laws or regulations.

Consent means written consent document which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Privacy Impact Assessment (DPIA) means tools and assessments used to identify and reduce risks of a Processing activity. DPIA can be carried out as part of privacy by design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Controller means natural or legal person, or any other body which determines the purpose (why?) and means (how?) of the Processing of Personal Data. For Rosti as a company group, this means each Rosti entity Processing the Personal Data.

Data Processor means natural or legal persons, or any other body which Processes Personal Data on behalf of the Data Controller. This means a Rosti entity Processing Personal Data on behalf of another Rosti entity or a third party Processing Personal Data on behalf of a Rosti entity.

Data Protection Officer (DPO) means the person appointed as Rosti's data protection manager with responsibility for Personal Data protection compliance. This position is currently held by Mari Lüdmois, dpo@rosti.com

Data Subject means a living, identified or identifiable individual, who's Personal Data is being or has been Processed. This includes any Rosti employee as well as our Business Partner's contact persons.

Business Partners are understood as prospects, customers, suppliers, consultants, service providers, contractors, members of board, candidates, agency workers, state institutions and other enterprises and institutions or individuals Rosti is in business relation with, regardless of form of relation.

Roles & Responsibilities

All employees, board member or other representative of Rosti shall Process Personal Data in compliance with the Policy and applicable laws.

All employees are responsible for reading, understanding and complying with the Policy, as well as any ancillary guidelines or similar adopted by Rosti from time to time, and making sure that they understand the contents thereof.

Rosti DPO

Rosti's DPO is responsible for overseeing the Policy together with Rosti Personal Data team and, as applicable, developing related policies and guidelines, ensure organisational arrangements, means and inter-functional collaboration to govern the Data Protection program throughout Rosti entities.

Data Controller

Each Data Controller is responsible to ensure compliance with the Policy and/or applicable Data Protection Laws and implement appropriate technical and organisational measures. Each Controller shall be able to demonstrate compliance with the Policy and/or applicable Data Protection Laws.

This is further set out in the GDPR Handbook on RostiNet.

Employees

Employees are responsible to:

- understand and comply with the Policy and Data Protections Laws;
- have a good understanding of how the Policy and Data Protections Laws relate to his/her position and/or responsibilities;
- seek guidance from his/her manager(s), local PDP responsible person or DPO when in doubt; and
- report any actual or suspected breach of the Policy or Data Protections Laws as guided in section Data Protection Breaches and Sanctions as soon as possible.

Managers

Managers at all levels are responsible for ensuring compliance with, and understanding of, the Policy and Data Protections Laws within their area of expertise and part of the organization, and in particular for:

- incorporating the Policy in local policies/procedures;
- fostering an open environment for employees to discuss possible violations of the Policy and/or Data Protections Laws;
- informing employees about the requirements set out in the Policy and/or Data Protections Laws and providing periodic training on how Rosti Process Personal Data, including induction training for new employees;
- conducting periodic risk assessments, in particular in relation to HR and IT, and ensuring that the risks of non-compliant Processing of Personal Data are minimised at first chance and included as appropriate in other risk assessments;
- tracking and demonstrating compliance with the Policy and Data Protections Laws and regulations; and
- taking appropriate action when breaches of the Policy and/or Data Protections Laws are suspected and/or identified, including notifying the DPO. This is further set out in Rosti's Guideline to manage Personal Data breaches on RostiNet.

Group Board of Directors and Managing Directors'

The Board of Directors of Rosti's parent company Rosti Group AB may request compliance reviews in relation to this Policy on a regular basis or at any time. This is further regulated by Rosti's internal governance documents.

However, day-to-day reinforcement, compliance reviews, information on how we Process Personal Data and other Personal Data related issues, is part of every managing director's responsibility, with the support of the DPO and Rosti's Data Protection team.

Business Partners

Rosti expects all Business Partners (and their sub-contractors, if any) to act at all times in a manner that is in line with the Policy when representing, performing services for or otherwise acting on behalf of Rosti.

Any transfer and/or out-sourcing of Personal Data to a Business Partners shall be governed by a written agreement, regulating the services performed and delivered to Rosti and the Processing of Personal Data.

Prior to engaging a new Business Partner, Rosti shall ensure the Business Partner's suitability, integrity and include a right to terminate the service agreement or co-operation in the event of misconduct or breaches of applicable laws or the Policy.

All Business Partner's must provide sufficient guarantees regarding appropriate technical and organisational measures to ensure that their Processing of Personal Data will meet the requirements of the applicable Data Protection Laws and ensure the protection of the rights of the Data Subject.

Principles for Processing Personal Data

Rosti is an international group, operating in various jurisdictions. As such, entities with Rosti will be required to comply with various Data Protection Laws in various countries, as well as Rosti internal policies.

Regardless of jurisdiction, we are required to

- Have control of all Personal Data that we Process;
- Be transparent on how we Process Personal Data;
- Proactively ensure compliance by reviewing, improving and adopting suitable technical and organizational measures on how we Process Personal Data; and
- Be able to demonstrate compliance with the applicable legislation.

All Processing of Personal Data shall be made in accordance with the following overriding principles.

Lawfulness

Whenever we Process Personal Data, it must be carried out in lawful manner in relation to the Data Subject. This mean that Personal Data may only be Processed if one or more of the following legal grounds are identified and achieved prior to initiating the

Processing. One of these legal bases is also required if the purpose of collecting, Processing and using the Personal Data is to be changed from the original purpose.

- **Contractual necessity**: Personal Data may only be Processed on the basis that such Processing is necessary in order to enter into or perform a contract with the Data Subject.
- **Compliance with legal obligations**: Personal Data may only be Processed on the basis that the Data Controller has a legal obligation to perform such Processing. The valid legal obligations will be set out in the applicable local laws.
- **Legitimate interests**: Personal Data may only be Processed on the basis that the Data Controller has a legitimate interest in Processing the Personal Data, provided that such legitimate interest is not overridden by the rights or freedoms of the affected Data Subjects. Unless a contractual necessity exists or compliance with legal obligations requires Rosti to Process the Personal Data, you are recommended to identify and document a legitimate interest. If necessary, please contact the DPO.
- **Vital interests**: Personal Data may only be Processed on the basis that it is necessary to protect the "vital interests" of the Data Subject (this essentially applies in "life or-death" scenarios).
- **Consent**: Personal Data may only be Processed on the basis that the Data Subject has Consented to such Processing. A Consent may be withdrawn at any time and should not be used in relation to Rosti employees as there is a presumption that an employee's Consent in relation to the employer is not freely given.
- **Additional local requirements**: Member States are permitted to introduce additional lawful bases for limited purposes connected with national law or the performance of tasks in the public interest.
- **Processing Sensitive Personal Data**: The Processing of Sensitive Personal Data is only permitted in case we have written explicit Consent, required for the fulfilled employment law, deference in connection with a legal claim or as otherwise permitted under the applicable law.

Fair and transparent

Being fair and transparent, and providing accessible information to Data Subjects about how we will use their Personal Data is a key element for the Policy. This mean that we need to:

- be open and honest about our identity;
- tell people why and how we intend to use Personal Data we collect about them, and give individuals appropriate privacy notices when collecting their Personal Data;
- handle their Personal Data only in ways they would reasonably expect;
- not use their Personal Data in ways that unjustifiably have a negative effect on them; and

- in communication relating to Processing to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Purpose limitation

Personal Data must be collected for specified, explicit and legitimate purposes and not further Processed in a way incompatible with those purposes. The purpose must be identified and stated prior to collecting the Personal Data.

In case existing Personal Data needs to be Processed for a different purpose not previously identified and stated, the new purpose and legal ground for such Processing needs to be identified and stated and the Data Subject shall be notified prior to any Processing.

Data minimisation

Personal Data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are Processed.

In other words, the principle of "Need to have only" shall be applied to all Personal Data Processing.

Accuracy

Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay.

Storage limitation

Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are Processed. Personal Data may not be collected in advance and stored for potential future purposes unless required or permitted by national law. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data shall be used.

Integrity and confidentiality

Personal Data must be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Maintaining appropriate security means guaranteeing the confidentiality and availability of the Personal Data by ensuring that:

- only people who are authorised to use the data can access it, and Personal Data may only be transferred to a Data Processor if they agree to contractual terms to put in place adequate measures to protect data that is shared, and
- authorised users should be able to access the Personal Data if they need it for authorised purposes.

Transfer of Personal Data

Personal Data may not be transferred outside the EU unless adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data are ensured. Each transfer of Personal Data between Rosti entities requires specific Personal Data transfer agreements based upon the European Commission's Standard Contractual Clauses.

We may only share Personal Data with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

We may only engage third party Processors if they have implemented sufficient security measures and are able to Process Personal Data in compliance with applicable law. In general, we may only share the Personal Data with third parties, such as our service providers if:

- they have a need to know the Personal Data for the purposes of providing the contracted services;
- sharing the Personal Data complies with the privacy notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract has been concluded.

For Processing governed by the GDPR, further instructions are set out in Rosti's guidelines on GDPR Handbook on RostiNet.

Confidentiality of Processing

Personal Data is subject to business secrecy and confidentially. Any unauthorized collection, Processing, or use of such data by employees is prohibited. Any Processing undertaken by an employee who has not been authorized to carry out such task as part of his/her duties is unauthorized. Employees may have access to Personal Data only as is appropriate for the type and scope of their work duties or the task in question.

Employees are forbidden to:

- use Rosti's Personal Data for other purposes then those stated when the Personal Data was collected,
- use Rosti's Personal Data for private purposes, or
- disclose Rosti's Personal Data to unauthorized persons

The obligation of business secrecy and confidentially of Personal Data shall remain in force even after employment has ended.

Business Partners shall always treat Personal Data as confidential information.

Security measures

Personal Data must be safeguarded from unauthorized access and unlawful Processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether Personal Data is Processed electronically or in paper form. Based on proper and continuous risk assessment and monitoring how Personal Data are Processed we set adequate and proportionate technical and organizational measures to safeguard Personal Data and the Processing.

Furthermore, to promote compliance with Data Protection Laws from the initial stages of new projects or initiatives involving Personal Data the principles of "**data protection by design**" and/or "**data protection by default**" must be applied. This includes that prior to the introduction of new methods of Processing (in particularly in relation to new IT systems) adequate and reasonable technical and organizational measures must be defined and implemented. These measures must be based on a risk assessment, and the classification of Personal Data: whether it is regular or sensitive Personal Data.

The department responsible for introducing the project or method must consult with Group IT and DPO.

Data Protection control and continuous improvement

Compliance with the Data Protection Policy and the applicable Data Protection Laws is reviewed on a regular basis.

To ensure continuous compliance and further strengthen Rosti's Personal Data Protection program, in particular data security, we are required to implement adequate risk assessment and auditing procedures to continuously review and update implemented technical and organisation measures.

If we use new technologies that might result in a high risk to the rights and freedoms of individuals, such as systematic monitoring of public areas (CCTV), we must conduction a Data Protection Impact Assessment. This DPIA shall be made by the responsible Rosti entity but approved by the DPO.

Procedures and regularity of all control activities, i.e. audits, risk assessment, DPIA and others compliance activities are described and set in PDP Compliance Governance.

Results of Data Protection controls, either global or local, will be reported to Board of Directors. Based on the audits, improvement activities shall be defined and implemented, which is natural part of annual planning procedure in Rosti.

Awareness of this Policy and how we Process Personal Data is an essential factor to ensure compliance with the applicable Data Protection Laws. We are therefore committed to provide regular training for all Rosti Employees to the extent necessary and relevant for their position and responsibilities.

Communication with Data Protection Authorities

If a Rosti entity receive a request, notification, order or other form of instruction by a Data Protection Authority or other form of law enforcement authority, the DPO and Rosti's Personal Data Team shall be notified immediately and be in charge of the subsequent communications.

Data Protection Breaches

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Rosti. For example, a hacker attack into Rosti's IT system, the loss of a laptop PC on a train, loss of a paper binder with payroll back-ups or an email contain Personal Data being sent to a non-permitted receiver.

All employees, board members and Business Partners are obligated to report any actual or suspected Data Protection Breach immediately to the local responsible person for data protection, the DPO by e-mail dpo@rosti.com and Rosti's IT Service Desk by e-mail servicedesk@rosti.com. In case immediate direct reporting to the above mentioned persons is not possible for Employee, they need to inform immediately their superior.

In cases of

- improper transmission of Personal Data to third parties;
- improper access by third parties to Personal Data; or
- loss of Personal Data

the reporting must be made immediately to DPO by e-mail dpo@rosti.com and by phone call (please see contact at the end of the Policy), so that any reporting duties under the applicable Data Protection Laws be complied with. For examples, the GDPR requires reporting to relevant Data Protection Authorities within 72 hours.

Complaint by Data Subjects

If you would like to lodge a complaint regarding how Rosti Process your Personal Data, please contact our Data Protection Officer.

Individuals have the right to lodge a complaint with the Swedish Data Protection Authority (Sw. *Datainspektionen, www.datainspektionen.se*) or with the Data Protection Authority of their country of residence if they believe that Rosti is in breach of the Data Protection Laws.

We must also comply with any rights given to the Data Subject or the relevant authorities and swiftly respond to utilizations of such rights. All contacts with the relevant authorities shall be communicated through the DPO.

More detailed information shared in GDPR Handbook.

Other non-compliance reports

All employees, board members and Business Partners are obligated to report any incidents or suspicious activities what might lead to breaches of the Policy and/or applicable law to the local responsible person for Data Protection and the DPO by e-mail dpo@rosti.com.

If the employee, board member and Business Partner does not feel comfortable in reporting by the means mentioned above, such employee may file an anonymous report through the whistle-blower function available at https://report.whistleb.com/RostiGroup in accordance with the procedures applicable to such function.

Rosti will protect employees who reject to take part in any violation of applicable laws and/or the Policy as well as employees who, in good faith, report suspected breaches of applicable laws or the Policy in accordance with the channels described above. Rosti prohibits all forms of intimidation or retaliation against such employees, even if the contents of the report, in subsequent investigations, proves to be mistaken. However, such leniency may not be applied if the employee filing the report does so in bad faith or if the reporting itself could constitute a criminal act.

Sanctions

Sanctions for company not complying with GDPR

Penalties for violating Data Protection Laws can be severe. Depending on jurisdiction, a company may be facing fines of MEUR 20 or 4 per cent of the annual world-wide turnover of the entire group (whichever is higher) or have had to agree to multi-million settlements.

Disciplinary Sanctions

Violations of the Policy and/or applicable Data Protection law, knowingly non-reported suspected breaches that employees knew about, and the reporting made in bad faith or maliciously can lead to disciplinary action including termination in accordance with applicable laws, regulations and collective bargaining agreements.

More information

Additional guidance and instruction, which are relevant to the Policy are available on Rosti's intranet and by contacting Rosti's DPO by e-mail: dpo@rosti.com or phone: + 48 781 820 583

Changes to the Policy

Rosti reserve the right to change the Policy at any time. The valid version will always be made available on Rosti's intranet.

Change register

Changed Chapter	Change description	Made by