Data Protection Policy – Ladó-Rec Ltd.

Aim of the Data Protection Policy

LADÓ-REC Waste Wholesale and Services Limited takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) very seriously. This policy sets out how Ladó-Rec Ltd. manages those responsibilities.

This policy therefore seeks to ensure that we:

1. are clear about how personal data must be processed and Ladó-Rec Ltd's expectations for all those who process personal data on its behalf

2. comply with the data protection law and with good practice

3. protect the reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights

4. protect the company from risks of personal data breaches and other breaches of data protection law.

Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored.

The responsible person for data protection is Miss. Mária Ladóczki and can be reached at drladoczkimaria@ladorec.hu.

The latest version of the Data Protection Policy can be accessed with the data privacy information at Ladó-Rec Ltd's website: www.ladorec.hu.

Principles for processing personal data

1. Fairness and lawfulness

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

2. Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected.

3. **Transparency**

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned.

4. **Data reduction and data economy**

Before processing personal data, you must determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken.

5. **Deletion**

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally.

6. **Factual accuracy**

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

Reliability of data processing

Collecting, processing and using personal data is permitted only under legal bases.

Customer and partner data

Personal data of the relevant customers and partners can be processed in order to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose.

Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospect that relate to contract conclusion.

Rights of the data subject

Every data subject has the following rights.

1.The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose.

2.If personal data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.

3.If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.

4.The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons.

5.The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation.

Confidentiality of processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized

Employees may have access to personal information only as is appropriate for the type and scope of the task in question.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

Processing security

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 data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented.

Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection and other controls.

Data protection incidents

All employees must inform their supervisor, responsible person for data protection immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data (data protection incidents).

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 required company reports must be made immediately so that any reporting duties under national law can be complied with.

Responsibilities and sanctions

The executive bodies of the company are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in the Data Protection Policy, for data protection are met.

Management staff are responsible for ensuring that organizational, HR, and technical measures are in place so that any data processing is carried out in accordance with data protection. Compliance with these requirements is the responsibility of the relevant employees

The managers must ensure that their employees are sufficiently trained in data protection. Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted and result in claims for compensation of damage. Violations for which individual employees are responsible can lead to sanctions under employment law.

Any data subject may approach at any time to raise concerns, ask questions, request information or make complaints relating to data protection or data security issues.

If requested, concerns and complaints will be handled confidentially.

Contact details for the responsible person of data protection:

Ladó-Rec Ltd.

HU- 6412 Balotaszállás, II. kerület 39.

E-mail: info@ladorec.hu

Tel: 0036309436794

Balotaszállás, 2020. január 01.