Privacy protection policy

1. Introduction

River Group (the **Company**) has implemented this policy to ensure compliance with the Act of 15 June 2018 no. 38 relating to the processing of personal data (the **DPA**) implementing Regulation (EU) 2016/679 (the **GDPR**). The Compliance Officer, “Head of Operational Excellence” is responsible for the compliance with this policy.

The entities in River Group use personal data in a limited way. There may be personal data collected as part of an order if we do business with a private person. Data collected is limited to what is absolutely necessary in order to process the order; name, address and in some cases social security number used for tax reduction (ROT). We also have names, telephone numbers and addresses to our business contacts. We strive to keep this information as updated as possible.

The Company shall review and where necessary update this policy. To the extent necessary, the Company shall implement supplementary technical and organisational measures to ensure compliance with this policy, the DPA and the GDPR. Such measures shall be proportionate in relation to the processing activities and appropriate to the risk related to the processing.

Based on the Company’s current processing of personal data, taking into account the nature, context, scope and purposes of the processing, the Company considers the processing unlikely to result in a risk to the rights and freedoms of natural persons.

2. Privacy principles

The DPA contains 7 privacy principles that form the fundamental conditions which the Company must follow when collecting, processing and managing personal data. The Company shall process personal data in accordance with these principles, further detailed below, and these shall be implemented in the Company’s supplementary procedures.

Lawfulness, fairness and transparency
“Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.”

The DPA requires that any processing of personal data should be lawful and fair. In order for processing to be lawful, personal data must be processed on a specific legal basis. The legal basis for the Company's processing activities will mainly be:

(i) law,
(ii) legal obligations to which the Company is subject,
(iii) it being necessary in the context of a contract or the intention to enter a contract with the data subject, or
(iv) the Company's legitimate interest.

The DPA furthermore requires that the processing must be transparent to the natural person of whom that personal data is processed and that it should be transparent as to what extent the personal data is or will be processed. The principle of transparency shall also ensure that the data subjects are familiar with their rights and enables them to utilise these rights.

Purpose limitation
"Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."

Any purpose for processing of personal data must be identified and described precisely. The principle of purpose limitation also indicates that processing of personal data is only permissible to the extent that it is compliant with the original purpose for which the data was collected. Processing for another purpose later on requires further specific legal basis such as consent.

Data minimisation
"Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."

The Company must ensure that only personal data which is necessary for each specific purpose is processed (in terms of the amount of personal data collected, the extent of the processing, the period of storage and accessibility).

Accuracy
"Personal data shall be accurate and, where necessary, kept up to date."

The Company shall ensure that every reasonable step is taken to ensure that personal data that is inaccurate, with regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitation
"Personal data shall 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."

This requires, in particular, ensuring that the period for which the personal data is stored is limited to a strict minimum. In order to ensure that personal data is not kept longer than necessary, time limits should be established by the Company for erasure or for a periodic review.

Integrity and confidentiality

"Personal data shall 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."

Personal data must be protected against unauthorised access using appropriate organisational and technical measures. The Company is responsible for ensuring that personal data is kept secure, both against external and internal threats, and appropriate measures must be implemented to ensure that personal data is protected with regard to confidentiality, integrity and accessibility.

Accountability

"The controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The principle of accountability sets out an obligation of the Company to be responsible for and to be able to demonstrate compliance with the DPA. In light of this principle the Company must be able to demonstrate compliance by e.g. documenting its decisions in writing in accordance with its internal procedures and guidelines.