# PRIVACY POLICY

**KLAPPIR GRÆNAR LAUSNIR HF.**

## 1. DEFINITIONS

Please navigate this section if you are having difficulties understanding some of the capitalized concepts found in this Privacy Policy.

**Automated Decision-Making (ADM):** when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

**Automated Processing:** any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Profiling is an example of Automated Processing.

**Company:** Klappir Grænar Lausnir hf. registered under the no. 630914-1080 whose registered address is at Austurstræti 17, 101 Reykjavík.

**Company personnel:** all employees, workers (such as contractors and agency workers), directors, members and others.

**Consent:** agreement 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 Controller:** the person or organization that determines when, why and how to process Personal Data. A Data Controller is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes, but our customers are the Data Controllers of the Personal Data Processed by us in the context of our services.

**Data Subject:** a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

**Data Protection Officer (DPO):** the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

**EEA:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

**Explicit Consent:** consent which requires a very clear and specific statement (that is, not just action).

**General Data Protection Regulation (GDPR):** the General Data Protection Regulation ((EU)

2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

**National Data Protection Laws:** the national data protection laws of the countries in which we operate.

**Personal Data:** any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behavior. The data obtained by our performance tracking system (Toolbox) is an example of Personal Data.

**Personal Data Breach:** any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organizational safeguards that we or our third-party service providers put in place to protect it. **The loss, or unauthorized access, disclosure or acquisition, of Personal Data is a Personal Data Breach. –** Please see Annex I, Security Incident Response Protocol, for information on how we respond to Personal Data Breaches.

**Privacy by Design:** implementing appropriate technical and organizational measures in an effective manner to ensure compliance with National Data Protection Laws.

**Privacy Guidelines:** the Company privacy related guidelines provided to assist in interpreting and implementing this Privacy Policy. The Privacy Guidelines may be found in annexes to this Privacy Policy.

**Processing or Process:** any activity that involves the use of Personal Data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring data to third parties.

**Pseudonymisation or Pseydonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

## 2. INTRODUCTION

This Privacy Policy sets out how Klappir Grænar Lausnir hf. ("we", "our", "us", "the Company") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Privacy 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 contracts, shareholders, website users or any other Data Subject.

This Privacy Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Privacy Policy when Processing Personal Data on our behalf and attend training on its requirements if requested. This Privacy Policy sets out what

we expect from you in order for the Company to comply with applicable law. Your compliance with this Privacy Policy is mandatory. Privacy Guidelines are available to help you interpret and act in accordance with this Privacy Policy. You must also comply with all such Privacy Guidelines.

This Privacy Policy (together with Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorization from the DPO.

## 3. SCOPE

We recognize that the correct and lawful treatment of Personal Data will maintain confidence in the organization and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines up to 2% of total revenue for failure to comply with the provisions of the GDPR.

All unit leaders are responsible for ensuring that Company Personnel comply with this Privacy Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPO is responsible for overseeing this Privacy Policy and, as applicable, developing related policies and Privacy Guidelines.

Please contact the DPO with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

## 4. PERSONAL DATA PRINCIPLES

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

a) Processed lawfully, fairly and in a transparent manner.
b) Processed in a manner that ensures its security using appropriate technical and organizational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage. – *See Articles 5 and 6 on Protecting Personal Data and Reporting a Personal Data Breach.*
*c)* Collected and processed for specified, explicit and legitimate purposes. – *See Article 7 on Purpose Limitation.*
d) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. – *See Article 8 on Data Minimisation*.
e) Accurate and where necessary kept up to date.
*f)* Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes of which the data is Processed. – *See Article 9 on Storage Limitation.*
g) Not transferred to another country without appropriate safeguards being in place.
h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data. – *See Article 14 on Data Subject's Rights and Requests.*

We are responsible for and must be able to demonstrate compliance with the protection principles listed above.

## 5. PROTECTING PERSONAL DATA

Personal Data must be secured by appropriate technical and organizational measures against unauthorized or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorized Processing of Personal Data and against the accidental loss of, or damage to, Personal Data.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

a) Confidentiality means that only people who have a need to know and are authorized to use the Personal Data can access it.
b) Integrity means that Personal Data is accurate and suitable for the purpose of which it is processed.
c) Availability means that authorized users are able to access the Personal Data when they need it for authorized purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect Personal Data.

## 6. REPORTING A PERSONAL DATA BREACH

Data Controllers are required to notify any Personal Data Breach to the applicable regulator and, in certain circumstances, the Data Subject.

We have put in place a protocol to deal with any suspected Personal Data Breach. Please see Annex I to this Privacy Policy or the "SECURITY INCIDENT RESPONSE PROTOCOL".

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact a member of the security incident response team. You should make your best effort to preserve all evidence relating to the potential Personal Data Breach.

## 7. PURPOSE LIMITATION

Personal Data must be collected and processed only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

## 8. DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for you job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's retention schedules (see Article x below).

## 9. STORAGE LIMITATION / DATA RETENTION SCHEDULES

Personal Data must not be kept in an identifiable form for longer than necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention schedules to ensure Personal Data is deleted after a reasonable time for the purposes for which it was first being held, unless a law requires such data to be kept for a minimum amount of time. Minimising data retention and having clear procedures in place to determine how and when to dispose of personal data is key to complying with National Data Protection Laws. Not only that, but a well-managed data retention plan can help us avoid the information overload and high storage costs resulting from the retention of unnecessary (and often redundant) data. Company department leaders are responsible for maintaining retention schedules for the Personal Data processed within the scope of their departments.

## 10. RECORD KEEPING

We are required to keep full and accurate records of all our data Processing activities.

We must keep and maintain accurate corporate records reflecting our Processing. First, we must keep records of the Processing of Personal Data we do as part of the service we provide our customers (Vinnsluskrá vinnsluaðila). Second, we must keep records of our processing of Personal Data relating to Company Personnel and Personal Data used for our own business purposes (Vinnsluskrá ábyrgðaraðila).

## 11. PRIVACY BY DESIGN

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organizational measures (such as encryption or access controls) in an effective manner, to ensure compliance with data privacy principles. In particular, we should look to apply such measures when we make changes to our software or develop new software altogether.

You must assess what Privacy by Design measures can be implemented on all software/programs/systems/processes that

Process Personal Data by taking into account the following:

a) the state of the art;
b) the cost of implementation;
c) the nature, scope, context and purposes of Processing; and
d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

## 12. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

Please see Article 1 of this Privacy Policy (DEFINITIONS) for the difference between Automated Processing and Automated Decision-Making.

Generally, Automated Decision-Making is prohibited while Automated Processing is permitted. However, Automated Decision-Making may be permitted if:

a) a Data Subject has Explicitly Consented;
b) the Processing is authorized by law; or
c) the Processing is necessary for the performance of or entering into a contract.

Therefore, should we develop an Automated Decision-Making process for our customers, we must make sure that the customer (Data Controller) has met one of the above conditions.

## 13. SHARING PERSONAL DATA

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee or contractor if the recipient has a job-related need-to-know for the information and the transfer of the information complies with any applicable cross-border transfer restrictions.

## 14. DATA SUBJECTS RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

a) withdraw Consent to Processing at any time;
b) receive certain information about the Data Controller's Processing activities;
c) request access to their Personal Data we hold;
d) prevent our use of their Personal Data for direct marketing purposes;
e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
f) restrict Processing in specific circumstances;
g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
i) object to decisions based solely on Automated Processing, including profiling (ADM);
j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

l) make a complaint to the supervisory authority; and
m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

We must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorization).

You must immediately forward any Data Subject requests you receive to our Company's DPO.

## 15. PRIVACY GUIDELINES

Our Privacy Guidelines may be found on our shared drives. They are currently the following:

SECURITY INCIDENT RESPONSE PROTOCOL

## 16. CHANGES TO THIS PRIVACY POLICY

We reserve the right to make changes to this Privacy Policy and its Annexes at any time without notice to you so please check back regularly to obtain the latest copy of this Privacy Policy. A folder storing this Privacy Policy has already been shared with you on Google Drive. We last revised this Privacy Policy on 14th of May 2018.

This Privacy Policy does not override any applicable National Data Protection Laws and regulations in countries where the Company operates.