PRIVACY POLICY

1. INTRODUCTION

1.1 Purpose

Green Resources AS and its affiliates ("Green Resources", "we", "us") is committed to data protection. It lies in the core of our business to keep data and communication confidential and to process it with care and diligence.

This privacy policy ("Policy") serves as a manual for our processing of personal data in accordance with Norwegian data protection law including the EU General Data Protection Regulation 2016/679 (GDPR). The terms used in this document shall have the meaning as defined in the GDPR.

This Policy has three sections:

- **Governing part**: Our data privacy organisation and governing principles.
- **Operative part**: Our data privacy guidelines and procedures for implementation of the governing principles and applicable data privacy laws. Some guidelines and procedures may be set out in separate documents, referred to in this Policy.
- **Controlling part**: Our routines for auditing and monitoring compliance with the data privacy guidelines/procedures and applicable data privacy laws.

2. GOVERNING PART

2.1 Privacy organisation

The legal responsibility for our data protection lies with **Green Resources** as company.

The **board** of Green Resources shall ensure that this Policy is appropriate.

The **CEO** of Green Resources shall ensure that this Policy is implemented in the business and that the employees are familiar with the content of it.

Green Resources does not have a data protection officer (DPO). We are not required to appoint a data protection officer, as we are not a public body, does not have as our core activities to regularly and systematically monitoring data subjects of a large scale, or does not have as our core activities to process special categories of personal data or data relating to criminal convictions or offences on a large scale.

2.2 Data protection principles

We will ensure that we process personal data in accordance with the data protection principles listed below.

We will integrate these principles both at the time of determination of the means to be used to process personal data and at the time of the processing itself (data protection by design).

Principle	Definition	How we comply
Data minimisation	Personal data must be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.	1. We will not collect personal data that we do not need. 2. We will limit the use of personal data in documents that we produce.
Data accuracy	Personal data will be accurate, complete and up-to-date.	1. We will verify collected data if we have reason to believe that they are inaccurate. 2. We will correct stored data if we have reasons to believe that they are outdated.

Data deletion	Personal data may be retained for no longer than is necessary for the purposes for which they are processed.	1. We will establish data retention periods. 2. We will delete or anonymise data when the retention period expires.
Data security	Personal data will be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.	1. We will use appropriate technical or organisational data security measures. 2. We will use systems adapted to technical developments and ensure that our suppliers also provide an appropriate level of data security.
Accountability	Each controlling entity is responsible for its compliance with data privacy laws.	1. We will document our data privacy guidelines and procedures. 2. We will monitor compliance with such guidelines and procedures.

2.3 Lawfulness

We may only process personal data to the extent we have a legal basis for the processing. The legal bases we rely on are documented in our Record of processing activities (see section 3.8 below). Below is a general overview of our approach to the legal bases.

For **non-sensitive data**, we may generally rely on any of following legal bases:

- Agreement. The data processing is necessary to fulfil an agreement with the data subject. *Example*: To handle a contract that we have with an employer or individual investor.
- Law. The data processing is necessary to comply with a legal obligation. *Example*: Collection of data for anti-money laundering purposes and storage of data for bookkeeping purposes.
- Legitimate interest. The data processing is necessary in order to achieve a legitimate interest which overrides the data subject's privacy interest. *Example*: Use of data for certain reporting or analysis purposes.
- Consent. The data subject has given its freely given, specific, informed and documented consent to the processing. *Example*: For marketing purposes (see section 3.2 below). We will generally not collect consents from our employees, as the imbalance between them and we as employer generally challenge the voluntariness.

For **sensitive data** (*i.e.* special categories of personal data), we will show particular caution. Sensitive data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as personal data relating to criminal convictions and offences). We may only process sensitive data if required for specific activities, and may typically rely on the following legal bases (in addition to the general legal bases in GDPR art. 6):

- Employment. The data processing is necessary for the purposes of carrying out obligations and exercising specific rights in the field of employment. *Example*: Use of health data on our staff to comply with our obligations as employer).

For **social security numbers**, we will limit the collection and processing to situations where we have an objective need for certain identification and the method is necessary to achieve such identification. *Example*: Use of social security numbers of our employees to report income to the tax authorities.

2.4 Purpose limitation

We may only process personal data for specified, explicit and legitimate purposes. The purposes for which we process personal data are documented in our Record of processing activities (see section 3.8).

We shall ensure that personal data are not further processed in a manner that is incompatible with the purpose for which they were collected. Subject to a case-by-case assessment, the following purposes will typically not be incompatible with the original purpose: communication, audits and investigations, dispute resolution, business development.

3. OPERATIVE PART

3.1 Data retention and deletion (GDPR art. 5)

We may only keep personal data for as long as required for the purpose for which they were collected.

The envisaged data retention periods will be reflected in our Record of processing activities. Here, we will also set out the reasoning for the retention periods.

We may use the following means of deletion: Automatic deletion, manual deletion, or anonymisation. If we select manual deletion, we will make sure that it is performed annually.

We will ensure that any processor storing data on our behalf adheres to the data retention periods we have established, and that we may require each processor to return to us or delete personal data after the term of the contract.

3.2 Marketing and profiling (GDPR arts. 6 and 21)

Our marketing communication, including sending newsletters and event invitations, must comply with the GDPR and relevant marketing legislation.

We will not send marketing communication by email unless:

- We have the recipient's consent, or
- We have an existing customer relationship (which gives us the possibility to rely on *legitimate interest* rather than the recipient's *consent).*

We currently do not perform profiling (evaluation of personal aspects of individuals to analyse or predict interests etc.) for marketing purposes. If we intend to do so, we will first consider whether applicable law requires us to collect consents or to allow the data subject to opt-out.

3.3 Cookies (GDPR art. 6 and Ecom Act art. 2-7b)

We use cookies on our website https://greenresources.no/. To comply with applicable law, we will publish a Cookie Policy on our website. We will also allow visitors of our site to opt-out by collecting their consent and/or respecting their browser settings.

We currently do not use cookies for marketing purposes. If we intend to do so, we will make sure to update our Cookie Policy made available on our website, and consider whether applicable law requires us to collect consents from the visitors of our site.

3.4 Transparency (GDPR arts. 12 – 14)

Our processing of personal data must be transparent. We will in a clear and plain language explain to the data subjects whose personal data we process, who we are, why we process their data and how the processing is carried out.

We shall make available a Privacy Notice (external) on our website to be transparent to our business contacts and the users of our website. Another Privacy Notice (internal) is available to our employees.

3.5 Data subject rights (GDPR art. 12 and arts. 15 - 23)

We shall respect the privacy rights of data subjects that we have data about. A right request from a data subject shall be handled without undue delay, and at latest within 1 month (which may be extended with 2 additional months where necessary).

The request shall be refused if we have reasonable doubts concerning the identity of the data subject, and the data subject does not upon request provide additional information that adequately confirms his/her identity. The request may also be refused if we can demonstrate that it is manifestly unfounded or excessive.

Below is our guidance for handling various rights requests that we may receive.

Privacy right	When does it apply
Right to access	Upon request from the data subject to receive a copy of its data.
Right to correction	Upon request from the data subject to have its data corrected.
Right to erasure	Upon request from the data subject to be forgotten, when: - the data is no longer necessary for the purposes for which it has been collected and used, - consent has been withdrawn (the deletion is limited to the data that was processed based on the consent), - the basis for processing is a legitimate interest and the data subject opposes the processing on the basis of his/her particular circumstances, or - the data is processed in an unlawful manner.
Right to restriction	Upon request from the data subject to have its data "freezed", when: - the data subject questions the accuracy of the data, and for as long as we need to verify and confirm the accuracy, - the data is processed in an unlawful manner and the data subject opposes deletion, or - the data is no longer necessary for the purposes for which it has been collected and used, but the data subject wishes to use it to establish, enforce or defend a legal claim.
Right to data portability	Upon request from the data subject to have its data transferred in a machine-readable format, when: - the processing is based on consent or contract, and the processing is carried out by automated means, and - only for data provided by the data subject or generated by the data subject's use of a service
Right to object	Upon request from the data subject to have the continued processing of its data ceased, when: - the basis for processing is a legitimate interest and the person opposes the processing on the basis of his/her *particular* circumstances, or - the data subject objects to direct marketing (then, the objection shall only cover the processing performed for direct marketing purposes).
Right to not be subject to automated decisions	Upon request from the data subject, when - the decision is made without human intervention, and - the automated decision creates a legal effect (such as a decision not to conclude a contract) or similar effect (such as to reject a job applicant).

3.6 Data protection by design and by default (GDPR art. 25)

Data protection by design. At the time of the determination of the means for processing and at the time of the processing itself, we will implement appropriate technical and organisational measures designed to implement the data protection principles (see section 2.2). If we ask service providers to perform system development or customization of tools, we shall require them to take due privacy considerations.

Data protection by default. We shall only use personal data which are necessary for each specific purpose. This means that we shall not collect excessive amounts of personal data, that we shall not process personal data for incompatible purposes, that we shall not store data any longer than required, and that we shall limit access to the data on a need-to-know basis.

3.7 Data processing agreement (GDPR art. 28)

Prior to engaging a processor (a service provider processing personal data on our behalf), we will verify that the processor provides sufficient guarantees to meet the requirements of applicable data protection law.

We shall conclude a data processing agreement (DPA) with all our processors. A DPA may form an appendix to another agreement entered into between us and the relevant processor. We may use the processor's DPA template, provided that it complies with GDPR art. 28(3).

When engaging important service providers, including service providers that are critical to the business, that process significant amounts of personal data, that process sensitive personal data on our behalf, or that uses cloud computing platforms, we will perform a risk assessment of the data security concerning the engagement of the service provider.

We try to limit the transfer of personal data to, or allow access of personal data from, a country outside the EEA, unless: it is a country approved by the EU Commission (see list here). When we do transfer data outside of the EEA we will always have legal grounds to do so. We will always enter into the EU standard clauses (SCC) with receiving third parties and conduct a transfer impact assessment, if required according to applicable privacy laws. In cases where we deem it necessary, we will also implement supplemental measures to ensure that the level of protection of the personal data is the same as in the EEA.

3.8 Record of processing activities (GDPR art. 30)

We will maintain a Record of processing activities for each of our data processing activities. The records shall be revised annually, and shall be updated when changes are made to our business.

The Record must, as a minimum, set out: (i) the controlling entity, (ii) the purpose of the processing, (iii) a description of the data subjects and the data categories; (iv) the categories of any recipients to whom the data have been or will be disclosed, (v) when data originating from a EU/EEA country are transferred to another country; and description of that third party and documentation of the privacy safeguards, (vi) the envisaged data retention periods, and (vii) a general description of data security.

The records will be revised annually, and will be updated when changes are made to our business.

3.9 Data security (GDPR art. 32)

We will ensure the data security of our processing systems, by the following measures:

Security criteria	Definition	How we comply
Confidentiality	Protection against unauthorised access or disclosure of data.	1. Our employees and business partners will be subject to adequate confidentiality obligations. 2. Our databases will be encrypted and subject to adequate access-control. 3. Our agreements with IT-vendors will include data security obligations. 4. Our physical facilities will be adequately protected against unauthorised access.
Integrity	Protection against unauthorised amendments to or deletion of data.	1. Our databases will be encrypted and subject to adequate access-control. 2. Key documents will have version control (revision history).
Accessibility	Access to data when needed.	1. Our agreements with key IT service providers will have adequate SLAs.

		2. Our main databases will be remotely accessible (VPN or similar).
Resilience	Business continuity is ensured	1. Our agreements with key IT service providers will have adequate SLAs. 2. We will have back-up of our data.

We will document our data security measures, such as by means of risk assessments. The documentation shall be maintained, such as to update it if the nature of our business changes or if we make material changes to our IT systems or facilities.

3.10 Personal data breaches (GDPR arts. 33 and 34)

We may potentially experience a personal data breach – a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples are hacking, communication of personal data to wrong recipients, or lack of access control. This applies also if the breach occurs at one of our service providers, as long it relates to our data.

We will handle the breach as follows:

Documentation: All security breaches must be documented. The documentation shall include a brief description of the circumstances of the breach and, if relevant, the consequences of the breach and the measures taken to mitigate it.

Notification. Depending on the privacy risk caused by the breach, as listed below, it may be necessary to notify the relevant data protection authority (DPA) and/or the affected individuals. Privacy risk may for instance be risk of discrimination, identity theft, fraud, financial loss, damage to reputation, loss of confidentiality, or social disadvantage. Examples may be where passwords, social security number, credit card data, or health data are compromised. We will follow the Norwegian Data Protection Authority's guidelines on personal data breach notifications.

- Low risk: If it is *unlikely* that the breach involves a privacy risk to the affected data subjects, no notification is required, but the breach must be documented internally.
- Medium risk. If it is *not unlikely* that the breach involves a privacy risk to the affected data subjects, the relevant DPA must be notified within 72 hours. The notification is to be made through a template Altinn form.
- High risk. If it is *likely* that the breach involves *high* privacy risk for the affected data subjects, individuals, also the affected data subjects shall be notified as soon as possible. However, notification to the data subjects is not required if appropriate security measures are implemented (such as encryption of the compromised data), subsequent measures are taken to ensure that high privacy risk is no longer likely to materialise, or notification would involve disproportionate effort (in the latter situation, a public communication, such as on the website, shall be made).

3.11 Data protection impact assessment (GDPR art. 35)

Where a processing operation, such as the use of new technology, is likely to result in a high privacy risk, taking into account the nature, scope, context and purpose, we will perform a *data protection impact assessment (DPIA)*. Due to the nature of our operation, we will generally not be required to perform DPIAs; however, we will make an assessment of whether it is required when we intend to implement new technology.

A potential DPIA must at least contain (i) a systematic description of the envisaged processing operation, (ii) an assessment of necessity and proportionality, (iii) an assessment of privacy risks, and (iv) measures to address the risks. Any performed DPIAs will be documented. We will follow the Norwegian Data Protection Authority's guidelines on DPIAs.

3.12 Training

We will make sure that all our employees who are involved in the processing of personal data are identified and have undergone training to ensure an efficient implementation of this Policy.

4. CONTROLLING PART

4.1 Audit

We shall review our Record of processing activities at least annually, and conduct ad hoc and periodic audits to verify compliance with this Policy.

Only anyone with the power to sign on behalf of Green Resources shall be entitled to notify to or communicate with the Data Protection Authority.

4.2 Documentation

This version of the Policy, and any privacy documentation referred to herein, shall be stored for at least 5 years.

4.3 Policy revision

Date	Version	Responsible
2022-01-10	Version 1	Hans Lemm