11-7-0 Information Security and Privacy Policy

Purpose
To ensure that personal data is processed in compliance with applicable regulatory requirements.
To provide information on how we handle personal data.

Scope
Personal data registered within the company.

Responsibility
The General Manager is responsible for ensuring that personal data processed by the company, including data relating to employees, contact persons at customers and suppliers, private customers, and other business relations, is handled in accordance with applicable legal requirements.

Implementation

1. Knowledge of the rules on personal data

Management and all employees who process personal data shall have knowledge of the rules governing the processing of personal data—specifically as described in this document and in the procedures. The level of knowledge shall be adapted to the individual employee's processing of personal data.

2. Mapping of the processing of personal data

All processing of personal data is documented in a separate register, which specifies, inter alia, categories of data subjects, the purpose of the processing, how the data is processed, and the legal basis for the processing.
The register contributes to ensuring compliance with the applicable rules for processing personal data. The register is only accessible to management, but all employees may request access.

3. Basic principles for the processing of personal data

There are six principles that apply to all processing of personal data:

1. Personal data shall be processed in a lawful, fair and transparent manner in relation to the data subject ("lawfulness, fairness and transparency"). Cf. Article 5(a) of the General Data Protection Regulation (GDPR).
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation"). Cf. Article 5(b) of the GDPR.
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization"). Cf. Article 5(c) of the GDPR.
4. Personal data should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay ("accuracy"). Cf. Article 5(d) of the GDPR.
5. 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 ("storage limitation"). Cf. Article 5(e) of the GDPR.

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (“integrity and confidentiality”). Cf. Article 5(f) of the GDPR.

4. Legal Basis / Lawfulness for Processing Personal Data

4.1 Legal Basis for Processing

There must be at least one of the following legal bases for all processing of personal data:

1. The data subject has given **consent** to the processing of their personal data for one or more specific purposes, cf. Article 6(1)(a) of the GDPR.
2. The processing is necessary for the **performance of a contract** to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract, cf. Article 6(1)(b) of the GDPR.
3. The processing is necessary for compliance with a **legal obligation** to which the controller is subject, cf. Article 6(1)(c) of the GDPR.
4. The processing is necessary for the purposes of the **legitimate interests** pursued by the controller—interest balancing—i.e. purposes relating to the controller’s interests or those of a third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, particularly where the data subject is a child, cf. Article 6(1)(f) of the GDPR.

The applicable legal basis for processing shall be specified in the record of processing activities.

Where processing is based on consent (see item 1), specific rules apply that must be documented.
Where processing is based on legitimate interests (see item 4), the balancing test must be specifically and documented in writing, see further below.

4.2 Employees

The processing of personal data is primarily based on legal obligations. Some processing is also based on legitimate interests. We need to document the information we process for personnel administration purposes for future reference. This constitutes a legitimate interest.
There is no equally effective way to achieve the purpose other than storing the personal data. Processing is therefore necessary.

Employees have an ongoing contractual relationship with the company. The personal data processed is linked to this relationship. The data primarily consists of information that employees themselves have provided. The data relates to matters that are naturally processed by an employer.

We consider that the company’s legitimate interests outweigh the interests of the employees.

4.3 Former Employees

The processing of personal data is based on a legitimate interest assessment. A need may arise (for us) to document employment relationships also after the employment has ended, for example in the event of a dispute with a former employee or a claim (occupational injury case). This may apply, for example, to documentation of the employment relationship for the purpose of fulfilling obligations under legislation or employment agreements. This constitutes a legitimate interest. It is not possible to achieve the purpose in another manner. Processing is therefore necessary.

The process consists of storing personal data for up to two (2) years. Information regarding the fact that the individual has been employed, the duration of the employment relationship, and work tasks may be stored for a longer period. Information shall not be disclosed to third parties unless the former employee requests it, for example in connection with references when applying for new employment.

We consider that the company's legitimate interests outweigh the interests of the employee.

4.4 Job Applicants

The processing of personal data is based on a legitimate interest assessment. We have a need to use personal data to assess job applications that are submitted. This constitutes a legitimate interest. It is not possible to assess an application without processing personal data. Processing is therefore necessary.

We request that applicants submit a minimum of information regarding name, education, work experience, references, etc. (CV). Applicants will often, in addition, provide further personal data that they consider relevant for the assessment of the application, for example contact information, family circumstances and interests. In interview situations, we ask questions in order to determine whether the applicant is suitable for the position. In some cases, we may use tests or seek references for this purpose. If it becomes relevant to proceed with the employment of the applicant, we may request additional information, as well as documentation supporting the information already provided. The provision of such information is voluntary.

We do not use the information for purposes other than assessing the application. We do not disclose the information to third parties. We may retain the information for up to six (6) months in the event that applicants believe their rights have not been respected.

We consider that the company's legitimate interests outweigh the interests of the applicants.

4.5 Contact Persons at Suppliers

The processing of personal data is based on a legitimate interest assessment. We have a need to maintain contact with our suppliers in order to follow up, inter alia, offers, orders and deliveries. This constitutes a legitimate interest. This contact can be most effectively maintained by contacting individual people directly. Processing is therefore necessary.

The processing is carried out in relation to the contact person's employer, which seeks to act as a supplier to us. In addition to the name, we process contact details such as telephone

number, email address, and employer information, all of which are primarily linked to the contact person's professional role and not to their private life.

The scope of the personal data processed is very limited. The process is connected to the supplier's business activities and not to the contact person's private affairs. The processing is clearly foreseeable to the contact person.

We consider that the company's legitimate interests override the interests of the contact person.

4.6 Contact Persons at Business Customers

The processing of personal data is based on a legitimate interest assessment. We have a need to maintain contact with our business customers in order to follow up, inter alia, offers, orders and deliveries. This constitutes a legitimate interest. Such contact can only be carried out effectively by communicating directly with individual contact people. Data processing is therefore necessary.

The processing is carried out in relation to the contact person's employer, which is a customer of the company. In addition to the name, we process ordinary personal data such as telephone numbers, email addresses and employers, all of which are primarily linked to the contact person's professional role and not to their private life.

The scope of the personal data processed is very limited. The processing is connected to the customer's business activities and not to the contact person's private affairs. Where consent is required under the Marketing Control Act, the contact person will have provided such consent prior to receiving marketing communications by email. The processing of personal data is clearly foreseeable to the contact person.

We consider that the company's legitimate interests override the interests of the contact person.

4.7 Other Contact Persons

The processing of personal data is based on a legitimate interest assessment. We have a need to maintain contact with public authorities, such as Norwegian Labor and Welfare Administration (NAV) and supervisory authorities, in connection with regulatory matters where the company may have rights and obligations. This constitutes a legitimate interest. In certain cases, such communication can only be carried out effectively by contacting individual people directly. Processing of data is therefore necessary.

We process and store names and contact details, and the processing of personal data is clearly foreseeable to the contact person.

We consider that the company's legitimate interests override the interests of the contact person.

5. Processing of Special Categories of Personal Data

The processing of special categories of personal data requires a legal basis in addition to those referred to in Section 4.

Special categories of personal data include: data revealing racial or ethnic origin, political opinions, religion or beliefs, or trade union membership, as well as genetic data and biometric data for the purpose of uniquely identifying a natural person, health data, or data concerning a natural person's sex life or sexual orientation, cf. Article 9 of the General Data Protection Regulation (GDPR).

Where such data is processed, the company shall ensure that an appropriate legal basis is established. For employees, data relating to health and, where applicable, trade union membership will be particularly relevant. Health data includes, for example, information relating to illness, injuries, and absence due to such conditions. A particularly relevant legal basis will be that the processing is necessary in the capacity of employer, for example in connection with follow-up measures and reporting to public authorities, or in order to facilitate appropriate working conditions.

The processing of personal data relating to criminal convictions and offences, or related matters, is subject to specific rules. The company shall ensure that it is familiar with and comply with such rules before processing such data.

6. Information for the Data Subjects (Privacy Policy) (cf. Article 12(1) of GDPR)

The company shall provide data subjects with the information required by law. Such information shall be provided in a privacy notice. All data subjects shall have access to the information relating to them. Information to employees is provided through the employee handbook, employment contracts, the intranet, or similar channels.

The information shall include, the name and contact details of the company, the purposes of the processing, the categories of personal data concerned, recipients of personal data (where applicable), information regarding any transfers of personal data to third countries, the retention period for the personal data, the data subject's rights to request access, rectification or erasure of personal data, information on how the company obtained the personal data, and the right to lodge a complaint with the supervisory authority.

Reference is made to Articles 13–15 of GDPR.

7. Rights of Data Subjects

The company shall respond to requests from data subjects without undue delay and, in any event, no later than one (1) month from receipt of the request. Any such requests shall be forwarded to the General Manager, cf. Article 12(3) of GDPR.

The company shall ensure that data subjects are able to exercise their rights. Reference is made to Articles 12–22 of GDPR.

8. Erasure of Personal Data (cf. Article 17 of the GDPR)

The company shall erase personal data without undue delay where it is no longer necessary for the purposes for which it was collected or otherwise processed. This should be reviewed at least once per year. The company's guidelines for erasure are set out below or in the records of processing activities.

9. Employees

Generally, the company retains personal data relating to employees for the duration of the employment relationship. Employees may request the erasure of personal data. Such requests shall be assessed on a case-by-case basis. Applicable legislation may impose requirements for longer retention periods.

10. Former Employees and Job Applicants

Reference is made to the above sections regarding the legal basis for the processing of personal data relating to these categories. Applicable legislation may impose requirements for longer retention periods than those stated therein.

11. Contact Persons at Suppliers and Customers

The company shall erase personal data when it becomes aware that the contact person is no longer employed by the supplier or customer, or where a new contact person has been appointed. The same applies where the supplier or customer relationship has been terminated.

The company may nevertheless retain such data for a longer period where it considers this necessary for the purpose of documenting its interaction with the supplier or customer. This may include, for example, matters relating to rights and obligations under contractual relationships. Applicable legislation may also impose requirements for longer retention periods.

12. Other Contact Persons

The company shall erase personal data when it becomes aware that the individual is no longer relevant for its purposes, for example where the individual is no longer employed by the relevant company, public authority or similar entity.

The company may nevertheless retain such data for a longer period when it considers this necessary for documentation purposes or continued contact with the individual or their employer. This may include, for example, matters relating to rights and obligations arising from contractual, regulatory or other legal relationships.

13. Data Protection Officer

The company has assessed whether it is required under the General Data Protection Regulation (GDPR) to appoint a Data Protection Officer.

The company has none or very few private individuals as customers. It does not carry out regular and systematic monitoring of data subjects on a large scale. For most categories of data subjects, the company processes primarily ordinary personal data such as name,

address, employer, email address and telephone number. Certain sensitive personal data relating to employees is processed.

The company has concluded that it is not subject to the requirement to appoint a Data Protection Officer, cf. Article 37 of the GDPR.

14. General Risk Assessment

The company shall carry out risk assessments relating to the processing of personal data. Such assessments shall enable the company to identify and determine appropriate security measures to be implemented, cf. Articles 24 and 35 of the GDPR.

The assessments shall consider the likelihood and severity of risks to the "rights and freedoms" of people, including risks of physical harm, material damage or financial loss, and medical harm. Examples of potential harm include discrimination, identity theft, damage to reputation, loss of social standing, unauthorized disclosure of confidential information, and unacceptable intrusions into privacy.

The record of processing activities shows the company:

- primarily processes ordinary contact data such as name, address, employer, email address, telephone number, etc.
- processes employee data that is necessary for the administration of employment relationships, including compliance with statutory obligations.
- has few or no private individual customers.
- has little or no personal data relating to children, and
- processes personal data as part of its ordinary business activities.

The company has not experienced any data breaches. Nor is it aware of any external parties having shown interest in the personal data it processes. The company therefore considers the likelihood of personal data breaches to be low.

Based on the nature and scope of the personal data processed, the company considers that the consequences of any breach would not be severe.

However, regarding certain categories of employee data, both the likelihood and the severity of potential breaches may be higher. The company has therefore established specific procedures for the processing of such data, including restrictions on access.

The company should conduct risk assessments in connection with changes that may affect information security, for example when procuring new IT services.

The results of risk assessments shall be approved by the person responsible for day-to-day processing activities within the company.

15. Information Security

In accordance with applicable law, the company shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with its processing of personal data. In doing so, the company shall consider the state of the art,

the costs of implementation, and the nature, scope, context and purposes of the processing, cf. Article 32 of GDPR.

The company's risks have been assessed at a general level in the section above.

On this basis, the company has implemented the following measures:

- A person has been designated with specific responsibility for information security:
  - **Title / Name: General Manager, Odd Gustav Kvalvåg**
- Unauthorized people shall be prevented from accessing personal data or the equipment on which such data is stored.
- The company's network shall be protected against intrusion from external networks by means of a firewall allowing only necessary data traffic.
- The company's network shall be protected against unauthorized use, for example by securing wireless networks.
- Additional safeguards shall be implemented for particularly sensitive data, such as medical certificates, employee evaluations, remarks and warnings.
- Employees shall receive training in the use of the company's IT systems.

16. Procurement of IT Services – Data Processing Agreements

As a general rule, the company will act as the **data controller** when procuring IT services from service providers. The company therefore remains responsible for ensuring compliance with applicable data protection legislation when purchasing IT services, such as HR systems or customer databases/CRM solutions.

Prior to procuring IT services, the company shall, inter alia, assess whether the service provider meets the security requirements set out in data protection legislation (cf. Article 32 of the GDPR). Reputable providers will typically be able to document compliance with such requirements.

The company shall also ensure that a **data processing agreement** is entered into, governing how the processor shall handle the personal data received from and processed on behalf of the company. Service providers will often have standard agreements that comply with applicable legal requirements.

Where the service provider transfers personal data to countries outside the EU/EEA, a lawful basis for such transfers must be established (cf. Articles 44–50 of the GDPR).

17. Personal Data Breaches

In the event of a **personal data breach** (e.g. cyberattacks or loss of personal data), the company shall immediately contact the supervisory authority in order to determine the appropriate course of action.

A "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed by the company.

In certain cases, the company shall notify the supervisory authority and, where applicable, the data subject. Notification to the supervisory authority (Datatilsynet) shall be made without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. Notification is not required where it is unlikely that the breach will result in a risk to the rights and freedoms of individuals, for example, where unauthorized access has been obtained to personal data that is already publicly available.

The company shall notify the data subject where the breach is likely to result in a **high risk** to the rights and freedoms of individuals. The company considers that its processing activities will only exceptionally give rise to such risk.

All personal data breaches shall be documented. This documentation shall include a description of the facts relating to the breach (what has occurred), the consequences of the breach, and the measures taken to mitigate its effects. Such documentation shall enable the supervisory authority to verify compliance with applicable legal requirements, cf. Articles 33 and 34 of the GDPR.

18. Data Protection Impact Assessment and Prior Consultation

The company shall carry out a **data protection impact assessment (DPIA)** where a planned processing operation is likely to result in a high risk to the rights and freedoms of individuals, including the right to privacy.

In assessing whether a DPIA is required, the company shall consider the nature, scope, context and purposes of the processing, as well as whether new technologies are used.
Examples of situations where a DPIA is required include:

- systematic and extensive evaluation of personal aspects based on automated processing.
- large-scale processing of special categories of personal data; or
- systematic monitoring of publicly accessible areas on a large scale.

In such cases, the company shall familiarize itself with the applicable requirements, including the obligation, where relevant, to consult the supervisory authority prior to processing, cf. Articles 35 and 36 of the GDPR.

19. Control, Updating and Revision of the Document

The company should update and revise this document on a regular basis. This is necessary, inter alia, because legal requirements may change, the company's processing activities may change, or experience may indicate a need to revise internal procedures.

For the same reasons, the company shall also regularly review and update its records of processing activities.

The General Manager is responsible for ensuring that the need for updates and revisions is identified and implemented in both this document and the related records. This shall be carried out as required.

The company has established separate procedures for internal audits and evaluation of systems and documentation.

19.1 Deviations, Root Cause Analysis and Corrective Measures

The company shall assess whether the processing of personal data complies with applicable data protection legislation and the procedures set out in this document. Where non-compliance is identified, the company shall determine how compliance can be improved. Both identified deviations and the corrective measures taken shall be documented in writing.

Where procedures are found to be insufficiently adapted to the company's operations, the company shall consider revising such procedures, cf. Section 19.