General Guidelines for Data Protection

For Bilpleie Holdco AS and its subsidiaries

1. Purpose and Scope

Bilpleie Holdco AS and its subsidiaries (*hereinafter referred to as "the company"*) processes personal data about its own employees, customers, suppliers, and other external parties. Such processing is governed by the **Norwegian Personal Data Act** *of June 15, 2018, No. 38*, and the **General Data Protection Regulation** (*GDPR*).

To ensure compliance with applicable regulations in daily operations, the company has implemented a set of procedures as described in this document, in accordance with *GDPR Article 24(2)*. The legal basis for processing personal data is found in *Article 6 of the GDPR* - **Lawfulness of Processing:**

1. Processing shall be **lawful only** if and to the extent that at **least one of the following applies**:

   a) The **data subject** has given consent to the processing of their personal data for one or more specific purposes.

   b) The processing is necessary for the performance of a contract to which the **data subject** is party or in order to take steps at the request of the **data subject** prior to entering into a contract.

   c) The processing is necessary for compliance with a legal obligation to which the **controller** is **subject**.

   d) The processing is necessary for the purposes of the legitimate interests pursued by the **controller** or by a **third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the **data subject**, particularly where the **data subject** is a child.

The purpose of this governance document is to define the general framework and instructions from the **CEO of Bilpleie Holdco AS and CEO's for subsidiaries** regarding how employees shall process personal data. **The objective** is to ensure a systematic approach to data protection regulations, so **that personal data is processed lawfully, securely, and responsibly.**

2. Responsibility

The CEO's of subsidiaries are responsible for ensuring compliance with data protection regulations (**data controller**). This governance document is relevant for the boards of subsidiaries, Management Teams, employees who process personal data as part of their job, those responsible for internal controls, audits, and other monitoring activities.

Overview of roles and responsibilities for personal data processing

Role	Responsibilities
CEO of Bilpleie Holdco AS **CEOs of subsidiaries**	• Overall responsibility for the processing of personal data in the company. • The CEOs of each subsidiary are responsible for monitoring, following up and notifying.
HR Manager	• Responsible for developing and implementing the operational follow-up of the company's data protection guidelines. • Monitor the developed guidelines and routines, make necessary corrections and provide support to subsidiaries. • Manages the daily follow-up of data protection efforts and related internal controls on behalf of the CEO's, including preparation for management review with risk assessments (high/very high), statistics on deviations, and reports from system owners. • Ensures the company's record of processing activities is maintained and updated when changes occur. • Responsible for reporting Data Protection Deviations to the Norwegian Data Protection Authority, notify affected Data Subjects when required. • Approve the disclosure of Personal Data only within the scope of the HR Manager's role.
System Owners, IT	• Overall responsibility for information security within the company and among subcontractors. • Ensures systems and services comply with requirements for built-in data protection. • Responsible for conducting risk assessments related to systems under their purview. • Enters into and follows up on data processor agreements.
Data Responsible (DR) *(Receptionists, Local Managers, Team/Shift leaders, Trade Union Representatives, Safety representatives, HR Assistant)*	• Keeps an overview of what personal data is processed within their area. • Ensures that new processing activities comply with regulations. • Handles and reports deviations.

Assessment of Need for Data Protection Officer (DPO):

*In accordance with GDPR Article 37, **Bilpleie Holdco AS** has assessed and concluded that it does not require the appointment of a Data Protection Officer (DPO), based on the criteria in the article.*

3. Definitions[1]

- **Data Controller**: The party who, alone or jointly determines the purposes and means of the processing of personal data *(in practice, the CEO*).
- **Data Processor**: An entity that processes personal data on behalf of the controller (*e.g., external vendors*).
- **Personal Data**: Any information relating to an identified or identifiable natural person, such as name, address, phone number, personal ID number, or bank account number.
- **Special Categories of Personal Data (Sensitive Data)**: Includes data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (*for identification*), health information, or data concerning a person's sex life or sexual orientation.
- **Data Subject**: A natural person to whom the personal data relates.
- **Data Responsible (DR)**: employees who have responsibility for ensuring that personal data processing in their area complies with GDPR requirements. reception, local management, team or shift leadership, trade union representatives, and safety representatives.

4. Security Objectives

The company shall protect personal data in terms of:

- **Confidentiality** – Information must not be disclosed to unauthorized persons.
- **Integrity** – Information must not be altered unintentionally or by unauthorized parties.
- **Availability** – Information must be available to authorized personnel when needed, and inaccessible to others.
- **Resilience** – Systems and the organization must withstand incidents and restore normal operations.

Personal data about subcontractors, customers, suppliers, and other external parties must be protected to safeguard both the data subjects and the company's own interests.

Employee's personal data shall only be accessible internally to those who require it for work purposes (e.g., payroll or HR staff).

5. Security Strategy

The company ensures security objectives by:

- Implementing access control in systems so that data is only accessible to authorized individuals.
- Providing staff with training and information on data protection and information security.

[1] ***GDPR Article*** *for more definitions: https://lovdata.no/static/NLX3/32016r0679.pdf*

6. Description

The company handles and processes personal data related to employees, customers (private individuals or dealers), suppliers, visitors to the company's website and other external parties. This data is vital for daily operations and must be managed securely to fulfill legal obligations and protect individuals' rights.

The company aims to be perceived as professional and trustworthy in its data handling. Relevant information should be readily available to those who need it, and it must be accurate and reliable.

All processing must follow the core principles outlined in **GDPR, Article 5**:

- lawfulness, fairness, and transparency;
- purpose limitation;
- data minimization;
- accuracy;
- storage limitation;
- integrity and confidentiality.

To meet these goals, the company maintains an internal control system ensuring both management and employees are aware of their responsibilities and equipped to handle personal data appropriately.

Key measures include:

- Strong leadership commitment to data protection and information security.
- Overview and risk assessments of systems and processing activities (record of processing activities).
- Adequate employee training.
- Clear roles and responsibilities.
- Defined system ownership.
- Deviation management.
- Monitoring activities.

7. Record of Processing Activities

According to **GDPR Article 3**0, the company must maintain a record of processing activities. This record must include:

- Types of processing
- Categories of personal data and data subjects
- Purpose
- Security measures
- Use of data processors
- Safeguards

The record must be updated regularly and reviewed annually in connection with the management review.

8. Requirements and Obligations

When processing personal data, the company is subject to various obligations under **the GDPR** and other applicable laws such as **accounting legislation**, **the Archives Act**, and the **Working Environment Act.**

Requirement	Reference	Procedure/Policy
Establish internal control	Article 5, 24	All routines and policies
Maintain a record of processing	Article 30	Data Processing Protocol and Record of Processing Activities
Ensure lawful processing	Articles 5(1), 44–49; Personal Data Act Chapter 3	
Inform data subjects	Articles 12–14; Personal Data Act Chapter 4	Privacy Policy for Employees
Deletion of personal data	Articles 5, 17	Erasure Policy
Ensure data protection by design	Article 25	—
Enter and monitor data processor agreements	Article 28	Policy and Procedure for Entering into and Managing Data Processing Agreements
Deviation handling	Articles 33, 34	Procedure for Handling Data Protection Deviations

9. Requirements and Obligations

9.1. Deviation Handling

A specific procedure has been developed for reporting and handling data protection breaches.

9.2. Internal Review

Routine and procedural owners shall conduct reviews annually to assess whether controls function as intended, are up to date, are followed in practice, and are known to relevant employees. Findings are reported as part of the management review.

9.3. Management Review

The **management teams** of Bilpleie Holdco AS subsidiaries **prepare** an **annual report** assessing whether internal controls are sufficient to ensure compliance with the GDPR. The report must be submitted to **the HR Manager,** who consolidates the findings and prepares an **overall report** on the subsidiaries of Bilpleie Holdco AS.

The purpose of the **reports** and **the review** is to monitor the achievement of data protection objectives and determine the need for corrective measures.

The review is based on:

- reported incidents with high severity;
- internal audit results;
- findings from internal reviews.

9.4. Training and Awareness

All employees involved in Data Processors selection, procurement, and contract management must receive training on this policy and the importance of data protection in third-party relationships.

9.5. Review and Updates

This policy will be reviewed annually or upon changes in legal requirements or processing practices.

ISSUED
by the **HR Manager** of Bilpleie Holdco AS

_____
Sandris Rakauskis
03.09.2025.

CONFIRMED
by the **CEO** of Bilpleie Holdco AS

_____
Glenn Brun Henriksen
08.09.2025.

Sandris Rakauskis
HR Manager
Telefon: 92283811
E-post: sandris@bilbyenbilpleie.no

bilpleie holdco as
Vassbotnen 13, 4313 Sandnes
NO 925 536326 MVA