Policy for Email Use and Access

For Bilpleie Holdco AS and its subsidiaries

1. Purpose and Scope

This **policy applies** to all employees of **Bilpleie Holdco AS** and **its subsidiaries** (*hereinafter referred to as **the "Company"***) who have been assigned a company **email address** and **mailbox**.

The purpose of this policy is to **ensure the proper use of, and access to, the Company's email systems.** This policy forms part of **the Company's** management system, as described in the **General Guidelines for Data Protection**[1].

2. Responsibilities

The **CEO** is responsible for ensuring that **the Company** adheres to overarching policies and guidelines. This includes compliance with data protection legislation and the establishment of clearly defined roles, responsibilities, and reporting lines.

The **HR Manager** is responsible for developing and implementing data protection practices.

The System Owners are responsible for ensuring that all current and future processing of personal data under their area of responsibility complies with GDPR and internal procedures.

All employees must be familiar with GDPR and internal routines and adhere to them. Questions should be directed to the immediate supervisor.

This **policy applies** to current employees, former employees, and external contractors or consultants performing work for **the Company**, both during and after their engagement. Provisions related to employees also apply to contractors, insofar as they are relevant.

The policy covers both the use of and access to **the Company's email system**. It equally applies to **the Employer's** access to an employee's personal area within **the Company's** IT network, as well as to other electronic communication systems or devices provided by **the Company** for work purposes (e.g., mobile phones).

3. Definitions

- **Mailbox**: An email account provided by the Company to an employee for work purposes.
- **Email address:** An electronic address assigned by the Company for business communication, linked to the Company's email system.
- **Data Controller**: The party that alone or jointly determines the purposes and means of the processing of personal data.
- **Data Processor**: A company that processes personal data on behalf of the data controller (**external service providers**).

[1] **General Guidelines for Data Protection,** *For Bilpleie Holdco AS and its subsidiaries, confirmed on 08.09.2025.*

- **Personal Data**: Any information that can be linked to an individual, such as name, address, phone number, national ID number, photo, license plate, location data, or bank account number.
- **Processing of Personal Data**: Any use of personal data, including collection, recording, compilation, storage, and disclosure, or any combination of these.
- **Data Subject**: The individual to whom the personal data relates.
- **Special Categories of Personal Data (Sensitive Data)**: Information about racial or ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, genetic or biometric data (used for identification), health data, and information regarding sexual life or orientation.[2]

4. Description

The Company's email and IT systems are provided as tools for work - related purposes. Use of the **email system for private matters should be kept to a minimum**. **The Company** is **not responsible for the loss of private emails** that are sent or stored in the system. The email system **must not** be used to distribute discriminatory, pornographic, or otherwise offensive material.

There is always a risk that emails may be misdirected. Users must be mindful of their language and should **always double-check recipients and attachments** before sending an email. All emails containing **personal data** or **special categories of personal data** must be **encrypted**.

Any information that might reasonably be considered **sensitive to the individual** (e.g., *personal financial status, social situation, national ID number*) must be treated as sensitive, particularly if it is uncomfortable for the individual if disclosed.

Incoming and outgoing business-related email must be stored continuously in the relevant designated location (e.g., project folders). If working on a project, all files and communications must be stored in the project's assigned area. Users are responsible for deleting emails that are no longer relevant or necessary.

Private or personal emails must be moved to a separate folder clearly marked **"Private"**. This must be done on an ongoing basis.

The Company will **not normally access** individual users' mailboxes. However, to protect a **legitimate interest**, including ensuring access to business - critical information, the Employer **may access a user's mailbox** if specific conditions are met. Whether the employer has a **legitimate interest** must be assessed strictly. Business needs may represent legitimate interests, but if the goal can be achieved by **less intrusive means**, access is **not permitted**.

The Company may access, search, or open a user's email **only**:

a) When necessary to maintain normal operations or other legitimate business interests, and/or

b) When there is reasonable suspicion that **the Employee** has seriously violated obligations under **the Employment contract**, or if the situation could lead to termination or dismissal.

5. Notice and Process:

[2] For further definitions, see **Article 4 of the GDPR**: https://lovdata.no/static/NLX3/32016r0679.pdf

5.1. The User must be **notified in writing** and given the opportunity to respond **before** access is granted, whenever possible.

5.2. The notice must **explain the basis for the access** and **inform** the **user of their rights**.

5.3. The User should be allowed to be present during the access process and may be assisted by a Trade Union Representative or other advisor.

5.4. At least **two company representatives** (*the CEO of the subsidiary and an HR Manager*) must be present. Technical support may also be involved.

5.5. If **the Employee** is unavailable, a **Trade Union Representative** or **Safety Representative** must be present.

5.6. A **written protocol** must be created and shared with **the User**.

5.7. If access is made without prior notice, the user must be informed **immediately after**, including:

a) The method used.

b) Which emails/documents were accessed.

c) The result of the access.

5.8. Access must be conducted in a manner that avoids altering data and ensures transparency and accountability.

5.9. If the review reveals no content that **the Company** is entitled to access, the mailbox and any opened documents must be **immediately closed**, and any copies **deleted**.

5.10. Before leaving **the Company**, employees must clean up their mailbox and data areas, ensuring that **business-related emails are stored or forwarded** to the appropriate person.

5.11. Email accounts and user profiles are deleted **within 14 days** of the employee's departure.

5.12. Incoming emails must **not** be reviewed **unless** the above access criteria are met.

6. Final Note

All employees are **obligated** to familiarize themselves with and follow the internal **security instructions**.

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