# Procedure for Handling Data Protection Deviations

*For Bilpleie Holdco AS and its subsidiaries*

## 1. Purpose and Scope

**The purpose** of this procedure is to **ensure** that **any deviations and incidents** related to the processing of **Personal Data** are **identified, documented, and handled** in a systematic manner, in accordance with the requirements of **Articles 33** and **34 of the GDPR**.

These provisions require the **Data Controller** to **notify the Norwegian Data Protection Authority** (*Datatilsynet*) in the event of a **Personal Data breach**. In certain cases, the **Data Subject(s)** must also be notified.

This procedure forms part of **Bilpleie Holdco AS** and **its subsidiaries** (*hereinafter referred to as "the Company"*) management system, as described in the **General Guidelines for Data Protection**[1].

## 2. Responsibilities

**This procedure** shall apply to **all employees** who discover, follow up, or are otherwise involved in a **Data Protection Deviation**. All employees shall familiarize themselves with this document, comply with its requirements, and report any **Data Protection Deviation** in accordance with the established routine. Questions regarding this procedure shall be directed to **the immediate CEO**.

The document owner **HR Manager** shall ensure that this procedure is kept up to date and that it is communicated and made available to all employees. The **HR Manager** shall **report Data Protection Deviations** to the **Norwegian Data Protection Authority** (*Datatilsynet)* in accordance with **Articles 33 and 34 of the GDPR** and shall notify **affected Data Subjects** when required.

**The CEOs** shall hold **the overall responsibility** for ensuring compliance with the **General Data Protection Guidelines** and shall **establish and maintain a management system with clearly defined roles**, responsibilities, and reporting lines. The **HR Manager** shall be responsible for developing and implementing the operational follow-up of the company's **Data Protection** guidelines and policies.

**The CEOs** shall ensure that all existing and new **Data Processing** activities within their area of responsibility are carried out in compliance with the **General Data Protection Guidelines**. Where such activities are performed by **external Data Processors,** compliance shall be ensured through appropriate **Data Processing Agreements (DPAs)** and continuous oversight of the processor's performance.[2]

## 3. Definitions[3]

[1] **General Guidelines for Data Protection,** *For Bilpleie Holdco AS and its subsidiaries, confirmed on 08.09.2025.*
[2] **Policy and Procedure for Entering into and Managing Data Processing Agreements.** For Bilpleie Holdco AS and its subsidiaries, confirmed on 08.09.2025.
[3] For further definitions, see **Article 4 of the GDPR**: https://lovdata.no/static/NLX3/32016r0679.pdf

- **Deviation:** any non-conformity or incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any personal data transmitted, stored, or otherwise processed.
- **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.
- **Logging**: The operational recording of events in a system, process, or activity (e.g., access logs, error logs, maintenance logs). Logging ensures traceability, accountability, and evidence of activities related to personal data processing.
- **Documentation:** Formal records such as procedures, guidelines, reports, registers, and corrective action plans, which describe and demonstrate how personal data is processed and how deviations are handled.
- **Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

**4. What is Data Protection Deviation?**

If a deviation entails a **breach of personal data security**, it must be assessed whether the deviation is of such a nature that the organization has a duty to notify the **Norwegian Data Protection Authority** (*Datatilsynet*).

According to **Article 4 (12)** of the **GDPR**:

*"'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 transmitted, stored or otherwise processed."*

A **Personal Data** breach can be categorized as follows:

- **Violation of confidentiality** – unintentional or unlawful disclosure of, or access to, Personal Data.
- **Violation of integrity** – unintentional or unlawful alteration of Personal Data.
- **Violation of availability** – unintentional or unlawful loss of access to, or destruction of, Personal Data.

A breach of **Personal Data** security may involve one or a combination of the above categories.

### *4.1. Typical examples of personal data breaches include (non-exhaustive):*

**a) Human errors or improper handling**

- Personal data is sent to the wrong recipient by post, email, or collaboration tools such as Teams.
- Correspondence is sent to the correct recipient but contains Personal Data about other individuals that the recipient is not authorized to access.
- Special categories of Personal Data are transmitted without adequate protection, for example, sent unencrypted by email.
- Employees access ("snoop into") Personal Data of others without a legitimate work-related purpose.
- Personal Data is mistakenly published online.
- Personal Data is lost, forgotten, or misplaced, either in paper format or on devices such as PCs, tablets, or USB drives, without sufficient protection and encryption.

**b) Failures in routines or procedures**

- No established routines exist for processing Personal Data.
- Insufficient routines for security testing result in IT systems being implemented without adequate protection of Personal Data.
- Lack of routines for reviewing security logs prevents the detection of Personal Data breaches.
- Inadequate access controls allow unauthorized individuals to access Personal Data.
- Weak routines for data disposal result in Personal Data not being properly deleted or destroyed after use.

**c) Technical errors or faults in IT solutions**

- System failures prevent security mechanisms from functioning as intended to protect Personal Data (e.g., encryption or access control failures).
- Missing security updates make IT systems vulnerable to hacking or data breaches, where Personal Data has been, or is likely to have been, accessed.
- Physical break-ins where digital media or paper documents containing Personal Data are stolen.

## 5. Internal Deviation reporting

All deviations shall be reported **immediately upon discovery**. The report shall at least contain information about:

- Time for when the deviation was discovered.
- Description of the deviation.

- Possible causes of deviation.
- What measures have been implemented to limit the consequences .
- Contact information about the person who discovered the deviation.

**Employees** who discover deviations **shall report to their immediate CEO**. **The CEO** who receives the note shall report **to the HR Manager**.

All reported deviations shall be documented using the prepared **Deviation Register in Plus Office (in the subsection Control Logs)**, ensuring that they are traceable, followed up, and closed in accordance with this procedure.

## 6. Handling Data Protection Deviations

**The Company's CEOs** and the **HR Manager** are responsible for handling the deviation, ensuring that the following steps are implemented:

- Immediate measures to stop the deviation and limit the extent of the damage.
- Examination of all aspects of the deviation.
- Implementation of necessary measures to prevent and counteract similar cases in the future.

The way a deviation is handled has a significant impact on the Risk Assessment and on the decision whether the **Norwegian Data Protection Authority** (*Datatilsynet*) and the affected **Data Subjects** shall be notified.

All decisions taken, by whom they were made, and all measures implemented must be documented in full.

## 7. Deviations Discovered by the Data Processor

If a **Data Processors** discovers a deviation they shall notify the the **Company's CEO (Data Controller)** without undue delay and assist in providing such information as is necessary for **the Company** to meet its reporting obligations, cf. the **Data Processing Agreement (DPA)**. The **CEO** shall immediately inform the **HR Manager**, who is responsible for assessing the deviation together with the CEO, and for carrying out further actions in accordance with this procedure.

The **Data Processor** shall **not notify** the **Norwegian Data Protection Authority** (*Datatilsynet*) or the **Data Subjects** directly. **Employees** who receive a notification from the **Data Processor** shall follow the procedure described in section **4: Internal Deviation Reporting.**

## 8. Notifying the Norwegian Data Protection Authority (Datatilsynet) and Data Subjects

### 8.1. When is notification required?

A **Personal Data Breach** may, if not handled properly and in a timely manner, cause physical, material, or non-material damage to individuals. Notification is required **only if the breach is likely to result in a risk to the rights and freedoms of natural persons.**

### 8.2. Risk Assessment of Personal Data Breach

Each deviation must be assessed thoroughly and concretely. The assessment shall establish, with reasonable certainty:

a) whether personal data was involved,

b) whether personal data may have been accessed, disclosed, altered, or lost, and

c) whether the breach is likely to have affected the rights and freedoms of the Data Subject(s).

When assessing the risk of a Personal Data Breach, the specific circumstances of the deviation must be reviewed, including the severity of the breach and its potential impact.

The following criteria shall guide the assessment of whether the risk is **low, medium, or high**:

- **Confidentiality, integrity, and availability**

  Breaches may involve unauthorized disclosure (confidentiality), alteration (integrity), or loss of access/destruction (availability). If several of these are affected, the risk level increases.

- **Categories of personal data**

  The sensitivity of the data is decisive. Special categories of personal data, or breaches involving multiple categories, generally entail higher risk.

- **Identifiability of individuals**

  Consider how easily individuals can be identified. If data is encrypted and encryption keys are securely controlled, the risk is generally low, in line with GDPR Article 32.

- **Severity of potential consequences**

  Consider possible outcomes for individuals: identity theft, fraud, discrimination, physical harm, or reputational damage. Such consequences normally indicate a high risk. If data has been mistakenly disclosed to a trusted third party who confirms secure erasure, the risk may be lower.

- **Characteristics of the data subjects**

  Breaches involving children or other vulnerable individuals/groups generally result in greater risk.

- **Number of data subjects affected**

  The more individuals affected, the greater the potential consequences and the higher the risk.

All Risk Assessments shall be documented. If it is concluded that a deviation does not require notification to **Datatilsynet** or to the Data Subjects, the justification for this conclusion shall be clearly recorded in the **Deviation Register**.

### 8.3. Responsibility for decision

The **HR Manager**, in consultation with the **CEOs**, shall determine whether the deviation must be reported to the **Norwegian Data Protection Authority** (*Datatilsynet*) and/or to the affected Data Subjects.

### 8.4. Decision framework and notification deadlines

a) **No personal data involved** → no notification required (document the assessment).
b) **No or low risk** → no notification required (document the assessment).
c) **Medium risk** → notify Datatilsynet within 72 hours; no notification to Data Subjects required.
d) **High risk** → notify both Datatilsynet (within 72 hours) and the affected Data Subjects without undue delay.

If not all information is available immediately, it may be provided in phases. Initial contact may be made by phone to alert **Datatilsynet**. If the breach is reported later than 72 hours, the reasons for the delay shall be documented.

If there is doubt as to whether Data Subjects should be notified, this often indicates that **notification should be carried out**.

All risk assessments, decisions, and notifications (or the decision not to notify) shall be documented in the **Deviation Register**.

### 8.5. Content of Notifications

**8.5.1. Report to Datatilsynet** shall include at least:

- Description of the breach.
- Root cause and how the breach occurred.
- How and when the breach was discovered.
- Number of Data Subjects affected.
- Categories of Personal Data involved.
- Relationship between the organization and the affected data subjects.
- Current location/status of the personal data.
- Likely consequences for data subjects.
- Measures taken or planned to address the breach and prevent recurrence.

Notification must be submitted via **Altinn.no** using form **DPA-01**. The reporter must have the role *Filler/Submitter* and log in with security level 2 or higher.

**8.5.2. Report to data subjects** shall be written in clear, plain language and include at least:

- Description of the nature of the breach.
- Contact details of the person responsible for Data Protection in the organization.
- Likely consequences of the breach.

- Measures taken or proposed to address the breach.
- Steps to mitigate possible adverse effects.

**9. Final Note**

It enters into force upon approval by the **CEO of Bilpleie Holdco AS** and shall be reviewed at least annually or whenever significant changes occur in legislation, organization, or processing activities.

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

_____
Sandris Rakauskis
**03.09.2025.**

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

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

_____
Glenn Brun Henriksen
**08.09.2025.**

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