

Compliance Analysis Report

Date: 10 November 2025, 12:20

Question: Can I store photos of employees for internal authentication?

Executive Summary

The inquiry about storing photos of employees for internal authentication touches upon critical aspects of **GDPR compliance**. The processing of personal data, including photographs, is subject to strict regulations under the GDPR. This report outlines the necessary legal principles and compliance requirements to ensure that the project adheres to EU law.

Compliance Score: 75/100

Detailed Analysis

GDPR Applicability: The General Data Protection Regulation (GDPR) governs the processing of personal data, which includes photographs of employees.

Article 9 - Special Categories of Data: Photos may be classified as sensitive data if they reveal personal characteristics. Processing such data is prohibited unless specific conditions are met, such as obtaining explicit consent.

Lawful Basis for Processing: You must establish a lawful basis for processing the photos:

Consent: Explicit consent from employees is required.

Contractual Necessity: If necessary for fulfilling employment contracts.

Legitimate Interests: Processing must be necessary and not override employee rights.

Data Minimization Principle: Only collect data that is necessary for the intended purpose. If photos are not essential for authentication, their collection may violate this principle.

Security Measures: Implement appropriate technical and organizational measures to protect stored photos against unauthorized access and breaches.

Specific, Actionable Next Steps

Obtain Explicit Consent: Ensure that you have informed, specific, and freely given consent from employees before storing their photos.

Define Purpose Limitation: Clearly articulate the purpose of storing the photos for internal authentication and avoid using them for other purposes without additional consent.

Establish Data Retention Policy: Create a policy outlining how long photos will be stored and the criteria for their deletion once they are no longer needed.

Implement Access Controls: Enforce strict access controls to limit access to the stored photos to authorized personnel only.

Conduct Employee Training: Provide training to employees on data protection and the measures in place to safeguard their personal data, including photographs.

Maintain Documentation: Keep records of processing activities, including the purpose of storing photos, the legal basis for processing, and documentation of employee consent.

By addressing these areas, you can enhance compliance with GDPR and mitigate potential legal risks associated with storing employee photographs for internal authentication.

Generated automatically by the Policy Checker (GenAI).