Sample Data Protection Impact Assessment (DPIA)

Below is a sample DPIA template for a fictional organization implementing a new employee monitoring system using biometric data.

1. Project Details

- **Project Name:** Employee Biometric Attendance System
- **Project Lead:** Jane Doe, HR Manager
- **Date of DPIA:** August 20, 2024
- **Project Summary:**
  The organization plans to implement a biometric attendance system that uses fingerprint scanning to monitor employee check-ins and check-outs. The system aims to enhance timekeeping accuracy and reduce fraudulent attendance practices. The system will store employees' biometric data (fingerprint templates) and will be integrated with the payroll system.

---

2. Describe the Data Processing Activity

- **Nature of Processing:**
  The biometric attendance system will collect and store fingerprint templates of employees. The system will authenticate employees when they check in or out, recording the time and linking it to their employee ID. The data will be automatically transferred to the payroll system for accurate calculation of working hours.
- **Scope of Processing:**
  The system will be used for all 500 employees across the organization's branches in USA. The biometric data will be stored on local servers at the head office and backed up to the cloud.
- **Context of Processing:**
  The system will be implemented as part of the organization's effort to streamline attendance tracking and reduce time fraud. All employees will be required to use the system daily. Data access will be restricted to the HR department and the IT team responsible for maintaining the system.
- **Purpose of Processing:**
  The primary purpose is to accurately track employee attendance and working hours to ensure fair payroll processing.

---

3. Assess the Necessity and Proportionality of Processing

- **Necessity:**
  The use of biometric data is necessary for ensuring that attendance records are accurate and cannot be easily manipulated. Other methods, such as manual sign-in sheets or RFID cards, have been found to be prone to abuse and errors.
- **Proportionality:**
  The collection and use of biometric data are proportionate to the intended goal of securing accurate timekeeping. The organization has ensured that only the minimal amount of biometric data (fingerprint templates) necessary for authentication is collected. The data will not be used for any other purposes beyond attendance tracking and payroll processing.

---

4. Identify and Assess the Risks

- **Risk 1: Unauthorized Access to Biometric Data**
  - **Likelihood:** Medium
  - **Impact:** High
  - **Description:** Unauthorized individuals, including internal staff, could gain access to biometric data, leading to privacy breaches or identity theft.
- **Risk 2: Data Breach During Cloud Backup**
  - **Likelihood:** Medium
  - **Impact:** High
  - **Description:** A breach in the cloud backup system could result in the exposure of sensitive biometric data to third parties.
- **Risk 3: Inaccurate Data Leading to Payroll Errors**
  - **Likelihood:** Low
  - **Impact:** Medium
  - **Description:** System errors or malfunctions could result in incorrect attendance records, impacting payroll accuracy and employee trust.

---

5. Proposed Mitigation Measures

- **Risk 1: Unauthorized Access to Biometric Data**

  - **Mitigation Measures:**
    - Implement strong access controls, including role-based access management (RBAC), to limit access to biometric data.
    - Use encryption to secure biometric data both at rest and in transit.
    - Regularly audit access logs to detect any unauthorized access attempts.
- **Risk 2: Data Breach During Cloud Backup**
  - **Mitigation Measures:**
    - Ensure that all biometric data backups are encrypted with robust encryption protocols.
    - Partner with a reputable cloud service provider that complies with GDPR requirements.
    - Conduct regular security assessments of the cloud backup environment.
- **Risk 3: Inaccurate Data Leading to Payroll Errors**
  - **Mitigation Measures:**
    - Implement validation checks to ensure accurate data entry and storage.
    - Test the system thoroughly before deployment to minimize errors.
    - Provide training to employees on how to properly use the biometric system and report issues promptly.

---

6. DPIA Documentation and Review

- **Documentation:**
  This DPIA and all related documentation, including the data flow diagrams, security protocols, and risk assessment reports, are stored in the organization's internal compliance management system.
- **Review Schedule:**
  The DPIA will be reviewed every six months or whenever there is a significant change to the processing activities. The next review is scheduled for February 2025.

---

7. Consultation with Data Protection Authority (If Necessary)

Based on the risk assessment, the organization does not anticipate a high residual risk that would require consultation with the Data Protection Authority. However, if new risks emerge during the implementation phase, the organization will seek guidance from the relevant authority.

Sign-Off

- **Project Lead:**
  Jane Doe, HR Manager
  Signature: ____________________
  Date: August 20, 2024
- **Data Protection Officer:**
  John Smith, DPO
  Signature: ____________________
  Date: August 20, 2024
- **Approved by:**
  Mary Johnson, CEO
  Signature: ____________________
  Date: August 20, 2024

This sample DPIA provides a structured approach to assessing the data protection risks associated with the implementation of a new biometric attendance system.