Data Protection Impact Assessment (DPIA)

System: Health Shield Portal
Organisation: Schools for Every Child Trust
Date: Nov 2024

Purpose

The purpose of this DPIA is to identify and mitigate any privacy and data protection risks associated with the use of the Health Shield Portal. This system enables Schools for Every Child Trust to register staff members for healthcare benefits, allowing Health Shield to reimburse staff for eligible healthcare expenses.

Project Overview

Health Shield is a benefits portal used to manage healthcare claims and reimbursements for Trust staff. Schools for Every Child Trust uses Health Shield to:

- Register staff members for healthcare benefits.
- Enable staff to submit claims for eligible healthcare expenses.
- Process reimbursements directly to staff for approved claims.

Key Information Processing Activities

- **Data Collection**: Information collected includes staff details (name, employee ID, contact information) and healthcare claims (date of service, amount, type of healthcare expense).
- **Data Usage**: Data is used to verify staff eligibility, process claims, and manage reimbursement payments.
- **Data Storage and Retention**: Data is securely stored within the Health Shield portal, in accordance with Health Shield's retention policies, and retained in compliance with applicable legal requirements.
- **Access Control**: Only authorized staff within the Trust and Health Shield have access to data, protected by secure logins and role-based access.

Risks and Mitigation

Risk	Description	Mitigation
Data Security	Risk of unauthorized access or data breach.	Health Shield uses encryption, secure access protocols, and regular audits to protect data.
Compliance with GDPR	Health Shield's data storage must comply with GDPR, particularly in data storage locations and transfer practices.	Health Shield operates in line with GDPR, ensuring data is stored within compliant jurisdictions.
Retention Policy Compliance	Data retention policies may differ between Health Shield's and the Trust's practices.	Ensure that Health Shield's retention policies align with the Trust's data management and legal requirements.
Subject Access Requests (SARs)	Staff may request access to, or deletion of, their personal data related to healthcare claims.	Health Shield provides tools to facilitate SARs, in line with GDPR.
Sensitive Data Handling	Healthcare claims data is sensitive and requires additional protection.	Health Shield implements data minimization, access restrictions, and regular security checks to ensure data privacy.

Roles and Responsibilities

- **Data Controller**: Schools for Every Child Trust
- **Data Processor**: Health Shield

Schools for Every Child Trust is responsible for the lawful and ethical use of staff data submitted to Health Shield, ensuring that data is handled according to Trust policies and GDPR requirements. Health Shield, as the Data Processor, is responsible for maintaining secure handling, storage, and processing of personal data in compliance with GDPR.