Case study: A medical scheme

Below, you will find a partially filled-in mini-DPIA received as a first draft from the controller, based on the example template in the accountability toolkit. While identifying risks and choosing controls is the controller's tasks, it is likely that they will often ask for your assistance. This **case study is partly based on some parts of the ECB's medical scheme**, but for reasons of timing is shorter than an actual DPIA would be. **Please approach this scenario as a blank slate** – please do not worry about whether things in this scenario work the same way as in the 'normal' Staff Regulations and JSIS.

Please take 30 minutes to discuss with your neighbours and identify some risks and controls to address them in point 9 below.

---

1. **Project name**

   EUI health insurance programme

2. **Validation/sign-off**

   [n/a yet, first draft]

3. **Review**

   Current status: V0.1 - initial draft by medical unit (responsible on behalf of controller)

4. **Summary**

   [n/a yet, to be added based on points 8 and 9 below]

5. **Reason for this DPIA**

   Our threshold assessment indicated that factors 4 (special categories of data: health data; suspicion of offences [fraud]), 5 (large-scale processing: all our current and retired staff plus dependents) and 7 (vulnerable DS: minor dependents of staff, staff/dependents with mental health issues) were met, so we should carry out a full DPIA.

6. **Main actors involved**

Medical unit:	Lead team, initial drafting for all parts
IT:	Input on technical aspects
Legal:	Input on contractual matters
DPO:	sent for consultation, waiting for input

7. **Description of processing**

   EUI has to provide its staff (both current and retired) as well as their dependents (collectively: beneficiaries) with health insurance, in accordance with EUI Staff Rules.

   EUI plans to use an external processor to run the insurance scheme. This is both to keep confidential medical information "at arm's length" from EUI as an employer of beneficiaries as well as because EUI doesn't have the appropriate skills and capabilities to

run such a scheme itself in a cost-effective way. In more detail, the main processing operations are the following:

EUI will inform staff about the whole processing and transfer personal data of beneficiaries to the provider in order to enrol them in the system.

The main process is settling reimbursement claims submitted by beneficiaries to the provider. The provider will assess the claim and reimburse them in line with the agreed rates for defined medical services. Beneficiaries can submit claims both on paper and electronically, using a web interface operated by the provider.

The provider will also operate a 24/7 helpline for beneficiaries, helping them with filing claims, to enquire about the status of submitted claims and to deal with any other questions.

Additionally, the provider will implement measures to detect fraudulent claims and ensure appropriate follow-up with EUI.

The provider will report back to EUI on how the insurance scheme is used (utilisation of financial envelope, trends…).

Data will be stored in the provider's data centre, located in the EEA.

EUI provides the funds for the insurance scheme.

[See flowchart on screen for data flow diagram]

8. Necessity and proportionality

EUI has to provide its employees (and dependents) with health insurance, based on EUI Staff Rules (see Articles X to Y); in that sense, it is a task assigned to EUI by Union law.

We only provide minimal information to enrol beneficiaries to the provider. Any additional information is provided directly by beneficiaries to the provider.

In its procedures for settling claims, the provider will follow data minimisation and enforce purpose limitation.

Procedures to detect fraud and ensure appropriate follow-up are necessary for sound management of the insurance scheme. In the past, we have become aware of attempts to defraud the predecessor system on multiple occasions. We will inform beneficiaries about this aspect of the system.

9. Analysis of risks and establishment of controls for identified risks

[see table on next page]

10. DS comments (if applicable)

We consulted the staff committee; they raised concerns about further outsourcing by the service provider, including to subcontractors outside the EU. We will include specific safeguards on this topic in the contract to be signed with the provider. We will re-consult them again once the programme will be more defined. We will also inform all staff about this project at a later stage.

11. DPO comments

[draft pending with DPO]

9. Analysis of risks and establishment of controls for identified risks

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity (gross, 1-5)	Likelihood (gross, 1-5)	Controls	Severity (residual)	Likelihood (residual)
1	General risk	Further subcontracting leading to loss of control by EUI and/or contractor	Security, purpose limitation	3	3	Contractual requirement: no further subcontracting without EUI's prior agreement	3	1
2	Electronic submission of claims							
3								
4								
...								
n								