



Workshop: A review of the guidelines on disciplinary matters DPO meeting 5 November 2015

Purpose of the workshop

This workshop is a gathering of experts in data protection who must reconcile data protection principles to data protection in practice in our daily work. We invite you to collaborate with us to pool our collective knowledge and experience to review our guidelines on **disciplinary matters**.

We propose that together we analyse three scenarios based on real cases. We are sure that this exercise will result in the best possible practical guidance document that will be useful in our daily work.

For each case, consider the following:

- How to ensure **accountability** (ensure, demonstrate and verify compliance);
- As a DPO, you have a specific role and you may face difficulties in fulfilling your task. This exercise is an opportunity to share these problems with other DPOs and to explore possible **solutions**.

CASE 1 - Harassment

Mr Dupont works in your institution. He is member of a union. In the last few weeks, one or more individuals have been regularly entering his office in his absence. They have been concealing his files, taking office supplies and putting cartoons and leaflets making fun of his trade union activities on his desk.

Mr Dupont complained about harassment to his hierarchy. The appointing authority decided to open an administrative inquiry against x.

Before starting their investigation, the investigators consult you to understand how to proceed from a data protection point of view. Among other things, they would like to set up a covert camera in Mr Dupont's office and to interview other staff in Mr Dupont's unit to try to identify the perpetrator(s).

CASE 2 - External activities

Mr Tiresias, a member of staff in your institution has developed an application "Pythia's imminent astrological responses" (PIAR), for people to be able to consult him about their future. He is suspected of carrying out this activity during working hours using office resources.

Mr Tiresias' Head of Unit and other colleagues have complained to Human Resources that Mr Tiresias is under-performing and disrupts the work environment because he is on the phone for most of the day talking about astrology.

The appointing authority decides to launch an inquiry. Ms Urania, in charge of the investigation, consults you and asks you a series of questions about how best to carry out the inquiry while respecting data protection principles. Ms Urania is determined to find concrete evidence and would like to access Mr Tiresias' hard drive and all the calls registered on his office telephone.

CASE 3 - Suspicion of fraud: timesheets

Mr Poirot is an official at the Commission. In his DG they have a flexitime regime which allows staff to take flexitime leave when they have enough time credit.

His Head of Unit, Ms Marple, suspects Mr Poirot of inflating the hours on his timesheets, since he takes a lot of flexitime leave although, in her opinion, he does not seem to work longer hours than others in her unit. Ms Marple decides

to check the access control system to verify when Mr Poirot enters and leaves the building in the morning, at lunchtime and in the evening. In addition, she explores the option of checking footage from surveillance cameras to verify when Mr Poirot's enters and leaves the building.

Suddenly, Ms Marple realises that her actions might have data protection implications and decides to involve you, the DPO.

Questions for each case

1. Do you think that the means of investigation contemplated in each case are appropriate?

What are the data protection requirements for these means?

Are there alternative ways to investigate?

2. What principles should the investigators keep in mind while collecting data during the inquiry?

List examples of data that must not be collected and of data that would be subject to specific precautions?

3. Should the institution inform the individuals involved in the investigation (the suspect, victims and any witnesses) about the ongoing inquiry?

4. What security measures (organisational, physical and electronic measures) would you recommend be put in place for the data collected?

5. What would be an adequate retention period for the data collected?

Would you consider different retention periods depending on the type of data?

6. What would you recommend to the institution if individuals involved in the investigation (the suspect, victims and any witnesses) request access to the investigation file?

7. The investigators want to share the findings of the investigation internally and with external entities as well. What conditions would make such transfers legitimate?