Case study
Mobile devices

Owe Langfeldt and Fidel Santiago
DPO meeting
27 October 2016
Scene setter

• DPO at Nameless EUI/EUA.

• Medium size entity: around 200 people.

• IT team (around 20 people).

• Corporate mobile devices for management (Smartphones and tablets)
  – Also, a BYOD programme in place.
Case 1

- IT Service Desk has contacted you.

- The Head of HR updated his/her corporate tablet according to the organisation’s security policy.

- After the update, the application Flopbox, which he/she installed, stopped working ➔ unable to access very important HR information.

- Flopbox is a cloud service to store and synchronise information between devices like a tablet and a desktop computer.
Case 1

What is your advice?
(we have 10’)


Case 1

• Mobile devices guidelines recommendations
  – R1: Involve the DPO regarding all the aspects of the introduction and use of mobile devices in the EU institutions.

  – R3: The concerned EU institutions should adopt an acceptable-use policy regarding mobile devices. This policy should also include user’s obligations regarding the life cycle of mobile devices.

  – R6: Adopt internal procedures for the handling of data breaches including notification by the controller to the DPO and to the EDPS.

  – V.5. A specific scenario: secondary storage of personal data via mobile devices

• And a link to use of the cloud, of course!!!!!!
Case 2

- A member of management would like to install Pokémon GO but
  - Unsure about if he/she is allowed to do it or not.
  - Concerned about the privacy loss.

- Two scenarios
  - BYOD scenario: it is user’s personal device.
  - Corporate smartphone.
Case 2

What is your advice?

(we have 10’)

Case 2

• Mobile devices guidelines recommendations
  – R3: The concerned EU institutions should adopt an acceptable-use policy regarding mobile devices. This policy should also include user’s obligations regarding the life cycle of mobile devices.

  – R7: When BYOD is allowed, the concerned EU institutions should:
    • Assess the risks to institutional and private personal data before introducing BYOD in the organisation.
    • Have a policy governing BYOD.

  – IV.2.1. Mobile device management ("MDM")
    • Application management: applications whitelists and blacklists;
Recap

– **R1**: Involve the DPO regarding all the aspects of the introduction and use of mobile devices in the EU institutions.

– **R3**: The concerned EU institutions should adopt an acceptable-use policy regarding mobile devices. This policy should also include user’s obligations regarding the life cycle of mobile devices.

– **R7**: When BYOD is allowed, the concerned EU institutions should:
  • Assess the risks to institutional and private personal data before introducing BYOD in the organisation.
  • Have a policy governing BYOD.
Thank you for your attention!

For more information:

www.edps.europa.eu
edps@edps.europa.eu

@EU_EDPS