EUROPEAN DATA PROTECTION SUPERVISOR

Mobile devices risk management and data protection

Fidel Santiago

DPO meeting

8 May 2015

The EDPS Strategy

2015-2019

Leading by example

Personal data in mobile devices

- Data relating to
  - Staff members EU institutions
  - Natural persons outside a working relationship with EU institutions
- Personal data may include:
  - Names, e-mail addresses, telephone numbers
  - Traffic and location data
  - IP addresses, cookies
- … as long as they can identify a natural person.
- Data for the management of the mobile devices themselves (“Mobile Device Management” solutions)

Data protection issues at stake

- Transfer to third countries, unintentionally
- No way to grant data subjects access to data on mobile devices
- Incorrect and outdated data on mobile devices, not respecting data quality
- Mobile specific processing (e.g. 3rd party apps) not registered and notified with the controller
- And, of course: **SECURITY!**

Accountability

- EU institutions: controllers as they determine the purposes and the means
- EU institution responsible for:
  - taking all measures necessary to comply with the Regulation
  - setting up the internal mechanism to demonstrate such compliance
- The DPO needs to be involved since the beginning to ensure the application of the Regulation

EDPS mobile guidelines

- Objective: to provide practical advice on the processing of personal data via mobile devices.

- Aimed at you (DPOs) as well as IT and IT security staff.

Approach

- Legal obligations related to mobile devices and personal data.
- Scope: data, operations, devices
- General approach to compliance
  - Identify specific risks related to mobile devices.
  - Identify appropriate safeguards.

Device types and usage patterns

- Device categories:
  - smart phones & tablets,
  - notebooks,
  - storage devices (USB sticks, disks, CD/DVD, …),
  - recording devices (cameras, MP3, …).
- Usage patterns:
  - synchronize email, calendar and contacts,
  - download business data,
  - scan, record, photograph, etc.,
  - remote access to desktop environment.

Risk management

- Data Protection Regulation Art. 22

- Risk management:
  - Risk assessment
  - Treatment or acceptance

Mobile devices risks (overview)

- Risk categories:
  - Application/OS
  - Vulnerabilities
  - Location
  - Communication
  - Device

Mobile devices risks (I)

- Application/OS:
  - mobile applications and/or the mobile OS (unlawfully) collecting and processing personal data;
  - customization by device manufacturers, carriers and/or OS developers leading to locked configurations and features;
- Vulnerabilities:
  - accidental loss of personal data due to security vulnerabilities;
  - intentional exploitation by hackers;
- Location
  - location services which may allow potential attackers to determine the location of the user;

Mobile devices risks (II)

- Communication related risks:
  - unlawful access to users' personal data by mobile device administrators;
  - illegal or unauthorized interception of the communications;
  - ‘man-in-the-middle’ attacks;
  - compromised network access;
- Device related risks
  - accidental loss of the mobile device;
  - theft of the mobile device;
  - physical tampering;

BYOD specific risks

- Reduced control by the corporate IT: security, configuration, applications, etc.
- Use of the personal device for intruding into the corporate network.
- Cross-access:
  - Corporate access to personal data.
  - Corporate information compromised through personal applications. E.g. cloud backup.

BYOD specific risks

- Reduced control by the corporate IT: security, configuration, applications, etc.
- **Ultimately, if the risk is considered too high, a ‘no go’ decision should be envisaged.**
- Cross-access:
  - Corporate access to personal data.
  - Corporate information compromised through personal applications. E.g. cloud backup.

Security measures

- Organizational measures
  - Updated security risk assessment
  - Information security policy
  - Acceptable use policy
  - Life-cycle management of the mobile device
  - Training
  - Organizational measures for BYOD
  - Security breaches/security incidents

- Technical measures
  - Mobile device management (“MDM”)
  - Other technical measures

Acceptable use policy

- Acceptable use policy:
  - approved uses and consequences of misuse,
  - responsibilities of the user and of the organization,
  - corporate information (personal data) allowed in the mobile device,
  - applications permitted to be installed and used,
  - policy regarding the use of cloud services,
  - monitoring of the use of mobile devices.

Org. measures for BYOD

- Assess the risks re: BYOD.
- The security and privacy controls defined are in use.

- Have a policy governing BYOD:
  - available before a user decides to go for BYOD;
  - “opt-in" with the policy, besides the mobile AUP, as a condition for BYOD permission;
  - “opt-in" user permission for systems management and monitoring of BYOD devices.

- Only devices approved.

- Provide users support for security, privacy and data protection.

Mobile Device Management

- Before implementing a MDM solution:
  - Assess the privacy impact.
  - Inform the users via the AUP of the MDM and its privacy impact.
  - Restrict the access to the MDM solution on a least-privilege, need-to-know basis.

EUROPEAN DATA PROTECTION SUPERVISOR

MDM requirements

- Security
- Device management
- Application management

- Application management:
  - remote application lock and wipe,
  - applications whitelists and blacklists,
  - enterprise application stores,
  - secure distribution of sensitive applications with appropriate controls against tampering,
  - per device applications inventory (both corporate and personal),
  - application security.
    - secure logs and audit trails of all sensitive BYOD activities,
    - backup and restore of data in the mobile device,
    - compliance check before accessing corporate resources,
    - data encryption both at rest (in the device) and in transit (communications encryption),

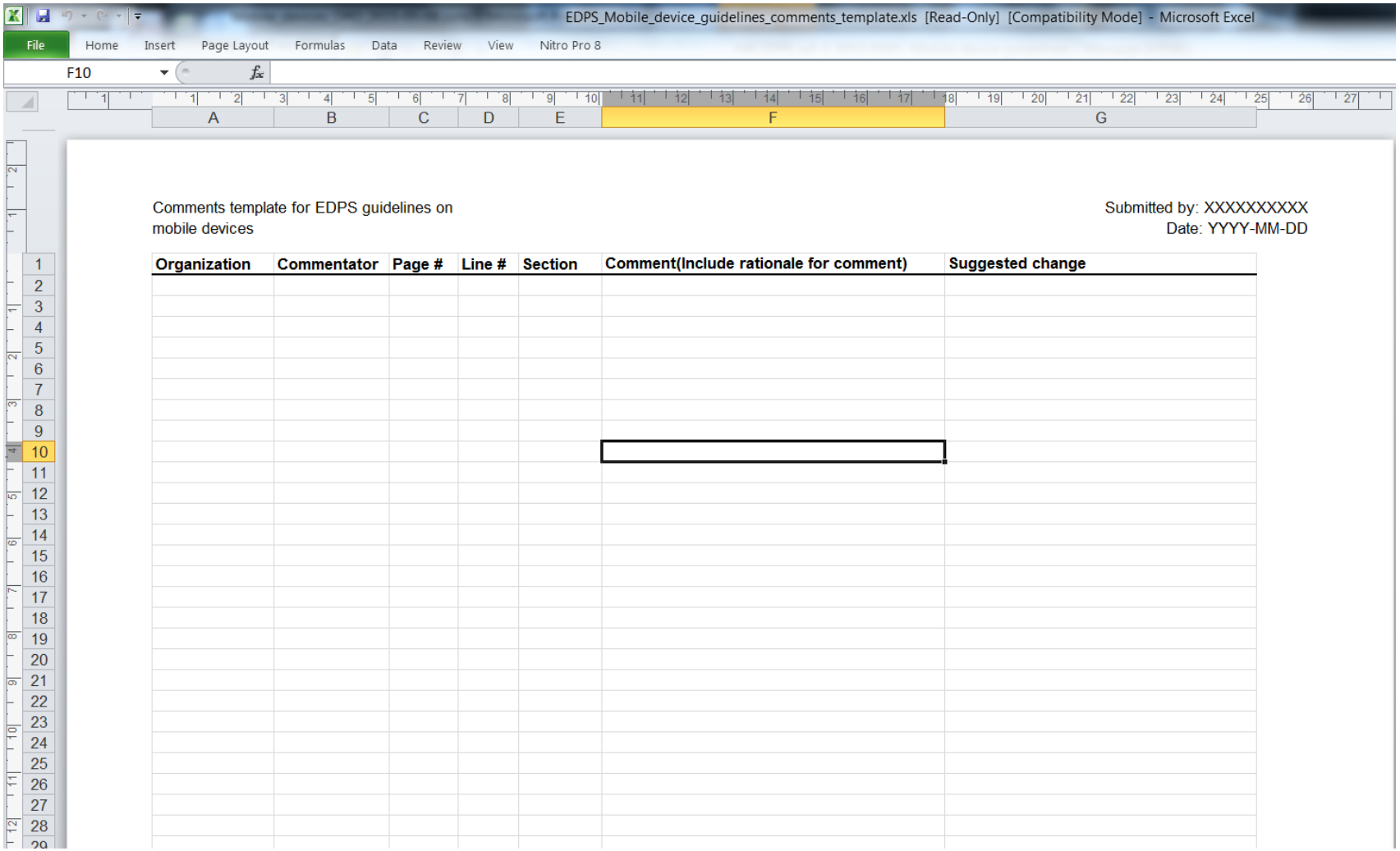
(Some) Other technical measures

- Develop, implement and test an encryption policy.
- Disable unneeded functionality (!!!!).
- Apply secure and privacy-friendly default configuration for mobile devices and applications.
- Only allow encrypted traffic between the mobile devices and the internal networks.

Current status and next actions

- Sent for your comments 6.5
  - Deadline 19.6
- Share internally with the relevant stakeholders
- Other networks (CII, CII security sg.)

Comments template



Comments template for EDPS guidelines on mobile devices

Submitted by: XXXXXXXXXX
Date: YYYY-MM-DD

Organization	Commentator	Page #	Line #	Section	Comment(Include rationale for comment)	Suggested change

Current practice in your organizations

- Risk management
- Information security policy
- Acceptable use policy
- Training
- BYOD
- Mobile device management (“MDM”)

EUROPEAN DATA PROTECTION SUPERVISOR

Recap

- Practical advice on the processing of personal data via mobile devices.
- For DPOs **and** IT/IT security staff.
- Risk based approach
  - Specific risks (including BYOD).
  - Safeguards.

Thanks!