EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on the protection of personal data in mobile devices used by European institutions

EDPS

December 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The popularity of mobile devices lies in the convenience, and increased functionality that they offer to users in addition to the efficient usage of IT resources. However, their use entails specific data protection risks due to the portability of these devices and the design of many of these devices for consumer use rather than professional use.

The aim of these Guidelines is to provide practical advice and instruction to the EU institutions and bodies on personal data and the use of mobile devices for work purposes to ensure that they comply with their obligations as set out in the Data Protection Regulation No 45/2001 (Regulation), applicable to the EU institutions.

Actively involving the Data Protection Officer, and where relevant the Data Protection Coordinators or Contacts, early in the process of planning the introduction of mobile device usage, will allow them to offer advice, suggest improvements and generally help the institution to ensure compliance with the Regulation.

EU institutions need to weigh up, the benefits of using mobile devices for each specific operation (case-by-case) and take into account the risks and invasiveness that their use may imply. This assessment should also consider the added functionalities and features of the mobile devices and the impact of introducing such devices on the security of IT infrastructure.

An acceptable-use policy on mobile devices is fundamental for regulating the relation between EU institutions and their staff. Where Bring-Your-Own-Devices are permitted, such a policy is even more important for clarifying the rights and obligations of EU institutions and their staff when private devices are used for work purposes.

The Bring-Your-Own-Device scenario is an increasingly common one since the benefits associated with mobile devices offer greater flexibility to the institutions and their staff on the way to work. However, they also imply specific risks to corporate and private data which must be assessed before being introduced; a specific policy for Bring-Your-Own-Device will also be required.

Security is one of the main enablers of data protection. To guarantee an adequate level of protection, EU institutions must implement a risk management process, assessing the security risks of using mobile devices for processing personal data; institutions must then implement measures to deal with the identified risks. These measures shall be both organisational, such as the adoption of information security policies, and technical, such as Mobile Device Management solutions.

To properly control mobile devices, whether they are the property of the EU institutions or privately owned, institutions should adopt written procedures for managing the lifecycle of mobile devices. Such procedures should take into account all operations that need to be performed on the device.

The measures mentioned above should reflect the policies adopted by the EU institutions and be designed with the principles of privacy by design and by default in mind. They should not collect and process more personal data than necessary (the data minimisation principle).

These Guidelines address the security aspects, as set out in the Regulation, of the processing of personal data by EU institutions via mobile devices. We recommend that this document be read in conjunction with the EDPS Guidelines on personal data and electronic communications in the EU institutions, which also address the issue of the monitoring of mobile devices by EU institutions.

While these guidelines are in principle aimed at the EU institutions, anyone or any organisation interested in data protection and mobile devices might find them useful; the Regulation (EC) No. 45/2001 is similar in many respects to the data protection Directive (EC) 95/46, which is implemented into the national laws of EU Member States, as well as to the national rules in Iceland, Liechtenstein and Norway.

I. Introduction

I.1. The Guidelines

1 When staff members of EU institutions, bodies or agencies ("EU Institutions") use mobile devices for their operational needs, they may be processing personal data of third persons on these devices. This could concern any individual who has any connection with the EU institutions, as a citizen using one of the EU's services, a staff member, a contractor, an applicant for EU funding, a member of the press or any other role. In these situations, it is the institution who is responsible for ensuring compliance with the data protection principles, in particular with Regulation 45/2001[1] ("the Regulation") in order to guarantee the rights to privacy and to the protection of the personal data. The responsibility rests with the EU institution, regardless of the provision of the mobile devices, whether they are provided by the EU institutions to management and staff with specific professional needs, or whether they are **private devices** which staff is allowed to use for professional purposes ("Bring Your Own Device" or "BYOD").

2 As the independent supervisory authority competent for the processing of personal data by the EU institutions, the European Data Protection Supervisor (EDPS) may among other tasks issue guidelines on specific issues related to the processing of personal data[2]. The present guidelines are **the result of a process** where the EU institutions have been consulted.

3 The guidelines are aimed at DPOs and DPCs within each EU institution, as well as IT and IT security staff and other administrative services concerned with the processes around professional use of mobile devices, and to all persons carrying responsibility for the EU institutions acting as controller.

4 The guidelines provide an analysis of the generic data protection risks related to the processing of personal data on mobile devices as well as recommendations and best practices which should help EU institutions to achieve a level of data protection compliant with the Regulation. While the purpose of the guidelines is to make it easier for EU institutions to fulfill their obligations, they do not take away any of the responsibility of the EU institutions applying them. EU institutions remain accountable for properly assessing and mitigating the risks related to their processing. The list of actions and measures recommended in these guidelines is not intended to be exhaustive or exclusive. While the EDPS will consider the best practices listed hereafter as a 'yardstick' when assessing compliance, the EU institutions are encouraged to perform their own risk analysis and choose appropriate measures accordingly. Their measures may be different from those presented in this document,

[1] Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, p. 1.

[2] In the exercise of the powers conferred under Articles 41(2) and 46(d) of the Regulation.

and the EDPS will assess the measures in place at an EU institution on the basis of completeness and effectiveness, not on adherence to the letter of the guidelines.

I.2. Technical background

5 Mobile devices, especially smartphones and tablets, pervade professional and private life. They are now ‘general purpose computing devices’ that run almost any application. In addition to voice calls and text messaging, they offer the ability to use internet services (social networks, content sharing, etc.) and feature many sensors providing an increasing amount of information linked to their users, such us location and an increasing number of environmental and personal parameters.

6 Smart mobile devices have had a profound **impact** on the way organisations work. Increasingly applications for these devices are being developed that are replacing workstations and laptops for some uses. Among the benefits are increasing employee satisfaction, cost savings, and the ability to accommodate for the increasing mobility need.

7 **Smartphones and tablets are not the only mobile devices** being used in organisations: portable storage, such as memory cards, USB sticks and hard disk drives also have had a great impact on data storage, transmission and security. The **security and privacy risks** implied by their use are high and should not be neglected.

8 In this regard, several **critical issues** have been identified:

- users of mobile devices for work-related reasons of EU institutions often process personal data **without being aware** that an action on the mobile device may involve a processing of personal data which is subject to the conditions and limits of the Regulation. The EU institutions may not realize that -since the data processing operations performed by their employees in the exercise of their functions are attributable to the EU institution- they remain liable for these processing operations, even though the operations might be only ‘transactional’ (e.g. forwarding an e-mail with the contact details of a new colleague);

- **‘smart’** mobile devices allow the use of software applications which interact with web resources. They exchange information via their network interfaces sometimes without the users or institutions being aware of this;

- when staff of EU institutions use their own private devices for professional purposes (for example, accessing and storing computer information) additional data protection issues are raised. The owner uses the same device for personal communications and for other purposes with apps of his choice installed. The EU institutions cannot exercise the same level of verification and control over the private devices that it has with institutionally-owned devices.

9 The principle of **accountability** is of paramount importance in the context of the use of mobile devices. This is particularly important due to the complexity of clearly defining the specific responsibilities for each and every actor involved according to the multiple possible use-cases. **Close cooperation between the data protection**

officers and the information security officers of EU institutions is strongly recommended.

II. Scope, methodology and structure of the guidelines

II.1. Scope

10 These Guidelines provide advice on compliance with privacy and data protection rules in the context of the use of mobile devices by staff members of the EU institutions for professional purposes. This advice does not prejudice a separate or specific policy that the EU institutions may consider with regard to their high level or political representatives.

11 These Guidelines cover both mobile devices provided by the EU institutions and those owned by its staff if used for professional purposes (BYOD). The term "**mobile devices**" includes phones, smartphones, tablets, laptops and netbooks, i.e. all devices enabling staff to work in mobility, as well as storage devices such as external hard drives and USB flash drives. These devices present common risks due to their ‘mobile’ aspect and small size although the security measures that can be implemented on/for them will be different. The main focus of these guidelines is on smartphones and tablets. For other mobile devices, subsets of the risks and the recommended measures apply.

12 While the use of mobile devices for professional purposes generally raises many IT security issues, risks concerning the information assets belonging to the EU institutions fall under the scope of these guidelines only insofar as the IT risks have an impact on personal data.

13 The following **issues** are addressed in these Guidelines:

- **general principles** for the processing of personal data by mobile devices by EU institutions;
- **risks for personal data** processed in mobile;
- **best practices** to protect personal data.

14 These Guidelines do **not address** the following scenarios and topics:

- staff using **devices owned by the EU institutions**[3] **for personal purposes**;
- staff use **only for personal purposes** of **private mobile devices** (even if brought to the workplace);
- risks for the EU institutions' interests and assets other than the ones related to the protection of personal data (e.g. protection of intellectual property or classified information);

[3] Since the use of the mobile device by a staff member **for his/her personal purpose** is not a processing done by or on behalf of an EU institution, it would fall **outside the scope of the Regulation**.

- processing of electronic communications data for detection of unauthorized use of mobile devices[4]; and
- digital forensics on staff members' mobile devices by competent EU institutions in the context of investigations[5].

II.2. Methodology

15 The process leading to these Guidelines was designed so that they are the result of a **structured open dialogue** with the EU institutions. The core steps/elements of this process are:

- the survey of 21 June 2013 as fact-finding exercise for collecting facts and reaching a better understanding of the EU institutions' position on the subject-matter;
- the Workshop held on 19 September 2013 on the topic and based on an orientation document preliminarily sent to the participants to the Workshop, where the EDPS also presented the survey results;
- the review of best practices on mobile devices security;
- the preliminary draft of the guidelines sent to EU institutions for their feedback, and
- taking into account such feedback, the finalisation of the guidelines.

16 These Guidelines will be revised by EDPS regularly re-engaging the EU institutions in an open dialogue process. A first review is intended to begin two years after adoption.

II.3. Structure

17 This document is structured as follows:

- Section III *Recommendations* presents the list of recommendations to implement based on the obligations laid out in the Regulation. The content of this section is the most relevant for both DPOs/DPCs and the IT/IT security personnel of EU institutions as it specifies the content a "mobile devices policy" should have.
- Section IV *Security measures to protect personal data processed in mobile devices* list some security measures based on best practices that the EU institutions can use to deal with the risks associated with mobile devices as those explained in section VI.
- Section V *Data protection issues related to the processing of personal data through mobile devices* discusses in more detail the different legal issues around the use of mobile devices defined in the scope of this document.

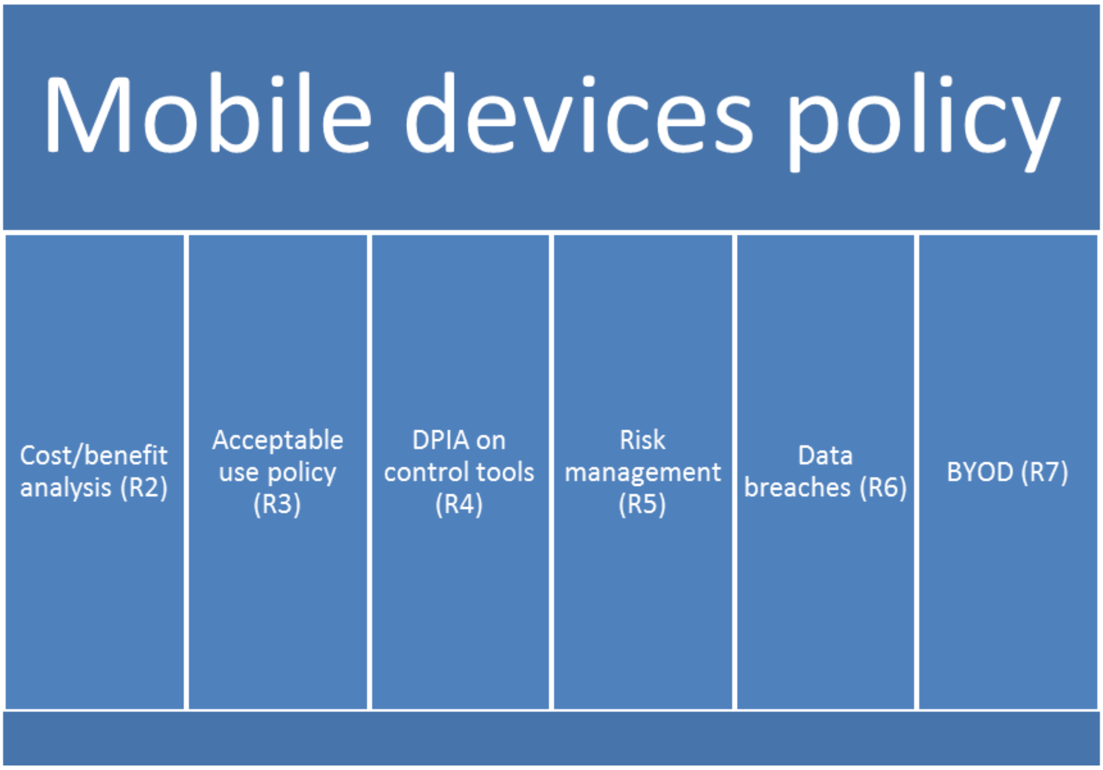
[4] Covered by the EDPS Guidelines "on personal data and electronic communications in the EU institutions".
[5] Ibid.

- Section VI *Risks for personal data processed by mobile devices* describes some of the risks associated with mobile devices.

> *Text in italics and inside a box represents examples and clarifications to the content of the text above.*
>
> *The sections are tailored to the needs of the different stakeholders required when dealing with the specific problematic of mobile devices: section III should be read by everybody as it describes the obligations emanating from the Regulation. Sections IV and VI contain the most relevant technical information of these guidelines with both security measures and risks associated with the use of mobile devices. Finally section V analyses the particular cases of processing personal data through mobile devices from a legal point of view.*

III. Recommendations

18 This section contains a set of recommendations which will help an EU institution demonstrate compliance with the Regulation when processing personal data through mobile devices. These recommendations can be understood as the different components of a *mobile devices policy* as per the following diagram.


Mobile devices policy
Cost/benefit analysis (R2)
Acceptable use policy (R3)
DPIA on control tools (R4)
Risk management (R5)
Data breaches (R6)
BYOD (R7)

R1: Involve the DPO regarding all the aspects of the introduction and use of mobile devices in the EU institutions. *(See section V.1)*

> *It is important that the DPO is involved from an early stage of the planning of the introduction of the use of the mobile device to ensure that the measures taken are compliant with the Regulation.*

R2: Perform a **case-by-case assessment of the benefits of allowing the use of mobile devices for specific processing operations taking account of the risks and invasiveness** that such use may imply *(See section V.1)*.

> *This assessment should take into account the added functionalities and features of the mobile device, such as enriching a contact list by adding photographs for the contacts with the camera of the mobile device.*
>
> *It also should include the impact of the introduction of mobile devices on the security of the current IT infrastructure. The introduction of insecure mobile devices might cause security challenges for an IT infrastructure that was designed relying on the assumption that all end-devices are secure and that the attackers are located outside the network. (See section V.2)*

R3: The concerned EU institutions should adopt an **acceptable-use policy** regarding mobile devices *(See section V.1)*. This policy should also include user's obligations regarding the life cycle of mobile devices.

R4: A **DPIA** should be performed on the monitoring and control tools used to guarantee the security of the mobile devices. This DPIA should address the main data protection principles and rules referred to in the Regulation, including lawfulness, necessity and proportionality; purpose specification and limitation; data quality, data retention; information to data subjects and data subjects' rights (access, rectification, erasure, blocking); data transfers and confidentiality of internal telecommunications networks or terminal equipment *(See section V.3)*.

> *Whenever a Data Protection Impact Assessment (DPIA) is carried out for a processing operation, the use of mobile devices for this processing operation needs to be taken into account. The DPIA could be carried out together with the IT security risk assessment, and in any case it should consider the related security risks (See section V.3).*

R5: Have a properly documented **risk management process** in place: controllers must take appropriate technical and organisational measures to safeguard the secure use of mobile devices. These measures should ensure a level of security appropriate to the risk presented, taking into account the available technical solutions and the cost of their implementation *(See section V.2)*.

> *In section VI, Risks for personal data processed by mobile devices, some of the risks associated with mobile devices are presented. These risks should be considered by the EU institutions when performing their risk assessment. Also, in section IV, Security measures to protect personal data processed in mobile devices, some best practices security measures are listed. The EU institutions should consider these measures as means to tackle the risks they will evaluate.*

R6: Adopt internal **procedures for the handling of data breaches** including notification by the controller to the DPO and to the EDPS *(See section V.4)*.

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 *(See section V.2).*
- Have a policy governing BYOD. *(See section V.1).*

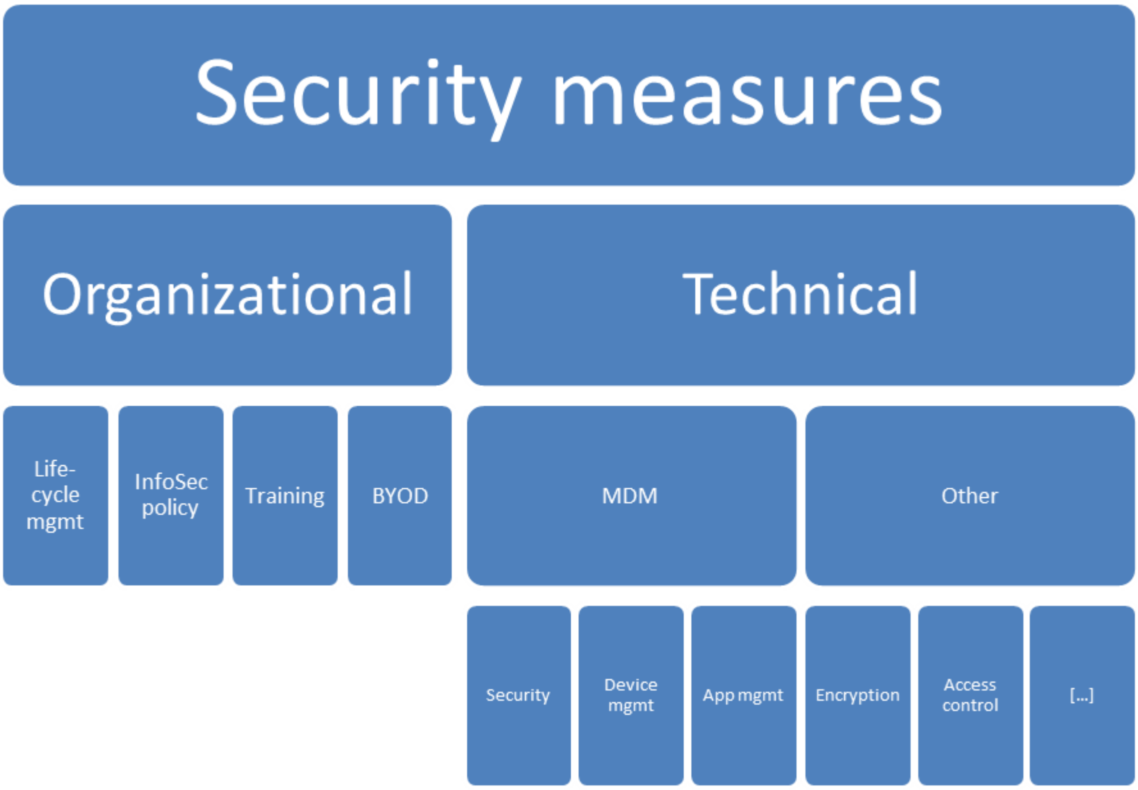
R8: In the case that there are local copies of personal data on mobile devices, it is also essential that the personal data stored on the mobile device is also made object of rectification, blocking or erasure when the data subject exercises the right to rectify the personal data that are inaccurate or incomplete or the right to block or erase unlawfully processed data. *(See section V.5).*

R9: The use of mobile devices as such is not, in principle, a reason to subject processing operations to prior checking to the EDPS pursuant to Article 27 of the Regulation *(See section V.1).* The need to submit a processing a processing operation to prior check by the EDPS should be analysed in the light of "purpose" of processing, in accordance with Article 27.2 of the Regulation.

IV. Security measures to protect personal data processed in mobile devices

19 This section provides a list of recommended organisational and technical security measures. This list is non-exhaustive and EU institutions may choose among them or adopt alternative measures addressing their specific needs on the basis of their own assessment of risks and needed level of security.

The following diagram summarizes these security measures:



IV.1. Organisational measures

20 The introduction of mobile devices into an organisation requires the establishment of a comprehensive policy including processes, training plans, management involvement, and procedures for dealing with incidents such as data breaches.

IV.1.1. Life-cycle management of the mobile device

21 The concerned EU institutions should adopt documented **procedures** for the managing of the whole lifecycle of mobile devices.

22 Such procedures should cover all relevant phases of the mobile device's lifecycle - from the purchase to the disposal- taking into account all operations that need to be performed on the device.

23 As part of this life-cycle management the EU institution will need to setup and maintain an **inventory** of mobile devices which includes for every device, at least:

- device identification and, where applicable, SIM identification;
- status of the device (e.g.: new, in maintenance, assigned, to be disposed of…);
- user to which the device is allocated, with begin and end time of allocation where appropriate (e.g. temporary allocated pool devices);
- ownership (institutionally-owned /BYOD).

24 An **asset disposal policy** is especially important for mobile devices. This policy should define the users' obligations. It must also provide for the retention of information as part of the full inventory of mobile devices about those devices marked for disposal. The choice of disposal methods should be based on the evaluation of the security vulnerabilities associated with each method of disposal and provide that devices are disposed of in a way that ensures in particular that all personal data is deleted in case the devices are removed.

IV.1.2. Information security policy

25 The concerned EU institutions should adopt an information security policy and specifically a **mobile device security policy** as well as the respective (clear and comprehensive) **privacy notice**.

> *The involvement of the management of the EU institution is paramount to the success of the policy which should reflect the security decisions and culture of the EU institution. All security policies should take into consideration data protection requirements.*

26 Security officers and DPOs need to be involved in the drafting of the security policies and of the privacy notices from the very early stages.

IV.1.3. Training

27 A **training plan** should be established to raise awareness on how to protect personal data on mobile devices when allowing their use to staff members.

This training is particularly important for management, since managers are likely to have access to the most sensitive data in the organisation. They also need to be made aware of their potential personal and financial liability for failure to respect the data protection obligations, similar to their responsibility under the Financial Regulation.

28 This training plan should follow the mobile device policies of the EU institution and may include the following scenarios and topics:

- Mobile device basic, security and privacy features;
- Business-related applications and services;
- Out-premises (travel) use and security;
- Private use of institutionally-owned devices;
- BYOD.

29 The training plan should be evaluated and updated periodically.

30 The training may be obligatory regularly as a ‘refresher course’ for every mobile device user.

IV.1.4. Organisational measures for BYOD

31 Establish organisational structures and processes ensuring that the organisation’s policies are applied to the devices (e.g. restrictions on the type or version of the device, type of operating system, configurations, etc.).

32 Provide users with support for configuring the devices with in line with the mobile device policies with respect to security, privacy and data protection.

IV.1.5. Security breaches/security incidents

33 Security procedures need to be in place to promptly and effectively respond to any security incident (such as the loss or theft of a mobile device). These processes need to take into account data protection requirements and involve the DPO.

34 Users need to be informed about how and where to report security incidents like the lost or theft of the device. Particular attention should be paid to the fact that users will typically not be in the office at the moment of the incident and thus adequate means for reporting security incidents should be set up covering all reasonable scenarios a user may find him/herself in.

IV.2. Technical measures

35 There are several risks concerning the processing of personal data. Most of the times the best, and even the only, solution to some of these issues is the careful evaluation

of the applications installed on a mobile device and the proper configuration of the operating systems as well as of the applications[6].

36 Managing and configuring devices, operating systems and applications was traditionally performed by dedicated professionals of the IT department. With the introduction of mobile devices, often used as BYOD, some of these tasks are now performed directly by the users, who are often neither IT specialists nor security/privacy experts.

37 To tackle this challenging situation, two approaches should be jointly used by the EU institutions concerned, namely:

- increase users' understanding and awareness of the data protection risks and on the possible countermeasures[7]; and
- use suitable "mobile device management" ("MDM") solutions which, as technical measures, address security and data protection requirements.

IV.2.1. Mobile device management ("MDM")

38 Mobile device management ("MDM") solutions can be used by the IT department of the EU institution to perform certain tasks related to the configuration and management of mobile devices for security purposes[8]. However, this capacity comes with increased responsibilities for the EU institution since this kind of software entails a -rather intrusive- processing of personal data (e.g. MDM may allow mobile devices to be tracked in real-time). Compliance with data protection requirements is therefore of essence.

39 The typical **set of features a MDM solution should include** is:

- Security:
  - enforcing device PIN/password use for accessing the mobile device, specific applications or containers as well as private keys;
  - remote device lock and wipe (of either all data on the device or of institutional information only);
  - detection of configuration change;
  - restrict user and application access to the device hardware;
  - restrict user and application access to native OS services;
  - secure logs and audit trails of management BYOD activities;

[6] More information can be found in the coming EDPS "Guidelines on the Protection of Personal Data processed through websites managed by European institutions and bodies" and the Opinion of the Article 29 Working Party on "Apps on smart devices", adopted on 27 February 2013.

[7] Where any particular risk of a breach of security exists, Article 35(2) of the Regulation obliges controllers to "*inform users of devices about the risks and possible remedies and alternative means of communications*".

[8] Although in the past MDM solutions were implemented for monitoring mobile phone use and billing purposes, in these guidelines we consider these solutions as having a security objective, hence not referring to MDM for use monitoring. As for this aspect, see the EDPS e-Communication Guidelines (footnote 4).

  - backup and restore of institutional information in the mobile device;
  - compliance check before accessing institutional resources;
  - data encryption both at rest (in the device) and in transit (communications encryption);
  - distribution and management of digital certificates.
- Device management:
  - centralized security policy enforcement;
  - over-the-air (OTA) distribution of software (applications and updates) and policy changes;
- Application management:
  - remote application lock and wipe;
  - applications whitelists and blacklists;
  - enterprise application stores;
  - secure distribution of applications with appropriate controls against tampering;
  - per device applications inventory (both institutional and personal);
  - application security.

40 MDM systems might not be capable to implement these features on all possible mobile devices but only a subset. This needs to be taken into consideration when deciding which mobile devices to allow.

41 In case a MDM solution is implemented the following measures need to be taken:

- Assess the data protection impact of the MDM solution.

As part of this assessment is important to identify what personal data the MDM solution collects and the purposes they serve, where and for how long it is stored, who has access to the data and the logging capabilities. The EU institution shall verify whether this information is strictly necessary for the envisaged purpose or there are less intrusive solutions.

- Inform the users via the acceptable use policy of the use of the MDM solution on their device, the type of information collected via the MDM and the purpose of this collection.

The MDM solution that the EU institution may put in place to ensure the security of the institutional data processed by the staff members on their personal devices can entail increased monitoring at work of the staff members by the EU institution. This monitoring could include, for instance, recording the geo-location of the mobile device or monitoring the internet traffic on the same device.

- Restrict the access to the MDM solution administrative console on a least-privilege, need-to-know basis[9].
- Evaluate the coverage of the MDM solution with respect to the full inventory of mobile devices and to other sources of information like applications or network logs.

IV.2.2. Other technical measures

42 An MDM solution by itself will not address all the risks implied by the use of mobile devices. The follow list provides technical measures that can be envisaged, depending on the specific risks of every EU institution. Some of these measures would benefit from an MDM solution for their implementation, although they do not require one to be functional. These security measures also need to be considered with specific devices in mind: encryption can be applied to portable memory storage, e.g. USB sticks, but not anti-malware software, at least in the USB stick itself.

43 T1: Design, implement and maintain a sandboxing, compartmentalisation or virtualisation solution to segregate private and institutional information.

> *Sandboxing provides a tightly controlled environment in a mobile device for applications to run in. With compartmentalisation an encrypted data store is created on the mobile device. The access to the information in the closed compartment requires authentication which is additional to any other authentication system currently applied in the mobile device.*

44 T2: Develop, implement and test an encryption solution which should ensure that personal data stored on the mobile devices (or, at least, in the 'institutional compartment' of the device, if a compartmentalisation/MDM solution is in use) are encrypted.

45 This solution may contain:

- The requirement for full disk encryption for all devices and of additional encryption for secure containers of applications;
- The requirement to use only standard encryption algorithms;
- The length of the encryption keys chosen must be appropriate to the security requirements.

46 T3: Develop, implement and test a backup solution to guarantee the availability of information stored only in the mobile device.

[9] *Need to know*: the user access to the information must be necessary for the conduct of user's duties. *Least privilege*: the rights of a user regarding certain information (read, write, etc.) must be the minimum needed to perform user's duties.

> *In most cases the mobile device is not the main storage for professional information and the configuration of the device is provided from a central repository which makes the backups unnecessary. On the other hand, personal data (like contact information) may only reside in the mobile device and may need to be backed up.*

47 T4: Design and enforce adequate user authentication to the mobile device including PINs and passwords to unlock the mobile device.

> *Users with access to sensitive information may have a second authentication factor in addition to the PIN/password.*
>
> *The mobile device should be locked and/or wiped after a predetermined number of unsuccessful PIN/password attempts.*

48 T5: Disable unneeded functionality.

> *E.g. disabling by default unnecessary or risky features, such as GPS, Near Field Communication (NFC), Bluetooth, etc. Disabling unneeded functionalities will provide a more secure mobile device thanks to reducing the attack surface an attacker may use to compromise the device and will make the mobile device easier to maintain because of the reduce number of components.*

49 T6: Apply secure and privacy-friendly default configuration for mobile devices and applications.

> *E.g.: automatic lock of the mobile device while inactive.*

50 T7: Ensure timely software updates of the mobile device and of the applications installed on it (whether using an MDM solution or not).

51 T8: Access to the internal networks of the EU institutions should only be granted after validating the network connection from a mobile device against the institutional directory and authorisations.

> *Device digital certificates and/or user digital certificates can be used to identify and authenticate the mobile device/user before granting access to the network.*
>
> *Two factors authentication may be implemented for connections regarding sensitive applications or information.*

52 T9: Only allow encrypted traffic between the mobile devices and the internal network of the EU institution.

> *Users need to be aware that VPNs (Virtual Private Networks) used for the encryption of the traffic between the mobile device and the internal network may redirect all traffic, including private communications, through the IT network of the EU institution.*

53 T10: Use industry-standard firewall and anti-malware applications on the mobile devices and block the access to the institutional network to devices devoid of such firewalls and applications and/or with outdated configurations. Both firewall and anti-malware application should be updated periodically (automatically or not, through an

MDM solution or directly with the vendor of the firewall or anti-malware application).

54 T11: According to the use policy, block any use of third parties applications to process the EU institution personal data, unless provided by the institution's policies and after an adequate assessment focusing on risks for personal data.

V. Data protection issues related to the processing of personal data through mobile devices

V.1. EU institutions as controllers accountable for data protection under the Regulation

55 In the context of the processing activities done via mobile devices it is particularly important to point out that personal data[10] is any information relating to any identified or identifiable natural person: this includes not only data relating to the staff of EU institutions, but also to natural persons outside a working relationship with EU institutions or agencies.

> *For example, devices could be used for mobile access to the user's institutional e-mail account, or to access a database containing personal data and downloading or synchronizing that information into the mobile device. Professional mobile applications could be installed onto the device to access information databases or web portals where different categories of personal data could also be available (for instance, a human resources management system).*
>
> *The personal data in question may thus include names, e-mail addresses, telephone numbers, traffic and location data, IP addresses and cookies, as long as they can identify a natural person. It should also be noted that the personal data may be processed under any form, such as in an e-mail which contains personal data, and with any technology, including Internet protocols. Even in the simplest case, for example when the device is used only for phone communications and SMS, traffic and contact data of the phone users and their communications partners will be processed. In addition, smart phones and tablets utilize a number of techniques that make it possible to identify and track individuals with regard to their physical location and in relation to how they make use of their device and applications (location-based services available on mobile phones and tablets collect location information that allows third parties to identify the precise whereabouts of users). Moreover, personal data of third persons (namely, persons outside the employment relationship with the EU institutions) may be contained in messages and stored calls, e.g. in a voice mail system.*

56 The EU institutions also need to collect and further process personal data for the management of the mobile devices themselves, and may often also install ad-hoc software on them. This is the case of the installation of so-called "Mobile Device Management" (MDM) solutions, which add functionality for security related data

[10] As defined in Article 2(a) of the Regulation. See also the Article 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data adopted on 20th June.

collection and interventions to the devices, connecting them with dedicated central control servers.

57 When a staff member of an EU institution uses a mobile device for work-related tasks upon instructions of the EU institution, this institution is the controller as it determines the purposes and the means of the processing of the personal data. The processing performed via the mobile device thus falls within the scope of application of the Regulation.[11]

58 Also in the 'BYOD' scenario, most problematic than the institutional one due to the reduced control the EU institution will have on the mobile device, the EU institution is still responsible for taking all measures necessary to comply with their obligations under the Regulation and for setting up the internal mechanism to demonstrate such compliance.

59 EU institutions should take care not to overlook that the processing via mobile devices needs to meet the same requirements and principles as processing operations in the 'traditional' desktop environment.

60 The staff member of an EU institution using his or her own device for the performance of work-related tasks (BYOD) has the obligation to implement the policies specifically adopted by the EU institution for this context.

61 In line with the principle of accountability, it is important that the DPO is involved from the early stage of the planning and management of data processing via mobile devices to ensure that the measures taken to mitigate or annul the data protection risks are appropriate and compliant with the Regulation.

62 The following **scenarios** can thus be considered the main examples of processing of personal data through the use of mobile devices:

- The processing of data by (staff of) EU institutions via mobile devices (by devices owned by the EU institution or according to the BYOD scenario) as a tool for data processing operations similar to those already performed by EU institutions in the traditional IT ('desktop') environment.
- The monitoring of staff members' use of the mobile device by EU institutions[12].
- The processing of personal data within the context of the deployment of MDM solutions.

63 In all of the above cases, the Regulation is applicable.

[11] It can be noted, as example of the application of the Regulation, that if - under this scenario - the mobile device is used to capture video or pictures, then the EU institution must address the issues raised in the EDPS thematic Guidelines on **video-surveillance**: at point 2.3.1 "Do the Guidelines cover devices other than CCTV systems?": "(…) using any other electronic device or system, fixed or **mobile**, also comes under the scope of the Guidelines if it is capable of capturing image data" (emphasis added).

[12] This scenario is out of the scope of these guidelines and addressed by the EDPS e-Communication Guidelines (footnote 4).

64 Recital 12 of the Regulation requires that "consistent and homogeneous application of the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data should be ensured throughout the Community". That includes the e-Privacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector). Without prejudice to specific provisions, these rules are a point of reference for EU institutions. In this regard it is important to consider the following: "In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay." - Article 4(3) of Directive 2002/58 (as amended by Directive 2009/136/EC). These rules are not directly applicable to EU institutions and bodies, however they might be considered as a good practise (see point V.4 below).

65 The Regulation lays down the conditions under which the processing of personal data may be lawful. The controller[13] must ensure that staff members do not use mobile devices for processing not covered by a **legal basis**[14].

66 The **necessity and proportionality** of the processing of personal data by mobile devices requires that the EU institutions perform a case-by-case assessment of the benefits of such tools compared to the risks and invasiveness that the processing may imply. This assessment should take into account the added functionalities and features of the mobile device, such as enriching a contact list with photographs taken with the mobile device.

67 The users of the mobile devices need to be **informed[15]** of the data processing being performed because of their use of mobile devices, whatever they are institutionally-owned or personal devices. Even more when personal data is collected and further processed for the management of the mobile devices themselves. The EU institutions should adopt an acceptable-use policy regarding mobile devices, which should include:

- clearly defined uses of the mobile devices approved by the EU institution,
- consequences of misuse of mobile resources,
- what institutional information and personal data is allowed to be stored and transferred to mobile devices,
- type and version of the mobile devices and operating systems approved,

[13] As stated in section V.1 the EU institution is the controller as it determines the purposes and the means of the processing of the personal data.

[14] Set out under Article 5 of the Regulation. In many cases, processing will be based on Article 5(a) which includes processing necessary for the management and functioning of the institution (recitals §27).

[15] Article 11 and/or 12 of the Regulation.

- what applications are permitted to be installed and used,
- the EU institution policy regarding the use of cloud services,
- return and disposal policy,
- a clear description of the responsibilities of the user and of the EU institution,
- under which conditions the monitoring of the use of mobile devices by EU staff members is allowed , and
- a notice on the personal data the user may collect and process via his or her mobile device.

68 The acceptable-use policy should be formally accepted by users before they can use mobile devices. In case the acceptable use policy changes, the new one should be promptly communicated to the users which will need to accept it again.

69 As for the BYOD scenario the policy governing BYOD should be easily available to all possible users of BYOD before they decide to use or not their own mobile devices for professional matters. This policy should include "opt-in" compliance with the policy, besides the acceptable use policy for all mobile devices, as a condition for BYOD permission; and "opt-in" user permission for systems management and monitoring of BYOD devices.

70 The configuration of the mobile device should reflect (“incorporate”) the rules (also pursuant to the principles of privacy by design and by default, and to the data minimisation principle). As for the implementation of the principle of purpose specification/limitation it is important to avoid ‘function creep’ (the collection and processing of data for not permitted secondary purposes), for example by excluding the installation of apps which are unnecessary for the work-related tasks and segregating office data from private data.

71 Regardless of the legal basis applicable to a specific processing operation, it is important to make reference -first of all- to the purpose of the data processing, and not to the technical device in use: the **use of mobile devices as such is not, in principle, a reason to subject processing operations to prior checking to the EDPS pursuant to Article 27 of the Regulation**. The need to submit a processing a processing operation to prior check by the EDPS should be analysed in the light of "purpose" of processing, in accordance with Article 27.2 of the Regulation.

V.2. Security obligation under the Regulation

72 Controllers must take appropriate technical and organisational measures to safeguard the secure use of mobile devices. These measures should ensure a level of security appropriate to the risk presented, taking into account any available technical solutions and the cost of their implementation[16].

[16] According to Article 22 of the Regulation.

73 This implies that controllers have to implement an **information risk management process** according to established principles of good practice. The first step of this process is the assessment of the risks, which should include an analysis of the use of mobile devices. This risk assessment will help determine the main security risks, and provide the basis for selecting the appropriate controls that must be implemented in order to reduce the risks to a level acceptable by management. The risk management process has to include periodical review of the risk assessment and the appropriateness of the safeguards and controls.

74 This information risk management process must be properly documented as a policy of the EU institution. It must also be regularly reviewed to ensure it remains effective, and aligned with new and changing business objectives. Staff members taking part in the process (especially in the analysis of the security risks) should not only be those dealing with security within the EU institution. Representatives from the 'core business' side (HR, core/operational business activities) and the DPO should also participate in discussions to ensure that the analysis takes into account the impact on all facets of the business.

75 The staff members concerned should be clearly aware of the main results of the information risk management process and of existing security risks, while management and key stakeholders may benefit from a detailed communication of the outcomes of this process.

V.3. Data Protection Impact Assessment (DPIA)

76 The EDPS recommends that when a Data Protection Impact Assessment ("DPIA") is carried out by the EU institutions, the use of mobile devices needs to be taken into account. In particular, the DPIA assessment should be carried out together with the IT security risk assessment, and in any case considering the related security risks.

77 The DPIA should be performed in particular on the monitoring and control tools used to guarantee the security of the mobile devices. This DPIA should address the main data protection principles and rules referred to in the Regulation, including the principle of lawfulness, necessity and proportionality of the data processing; purpose specification and limitation; data quality, data retention; information to data subjects and data subjects' rights (access, rectification, erasure, blocking) and data transfers.

V.4. Communication of data breaches

78 The EDPS recommends the EU institutions to adopt internal procedures for the handling of security and data breaches that foresee in particular the notification of the occurrence of such events by the controller to the DPO.

For example, in case of loss or theft of the mobile device entailing a personal data breach, the staff member should report the event internally according to the EU institution's policy on the handling of security and data breaches. The DPO should assess and document the breach and the measures taken in reaction for future assessment and verification and consider whether it is appropriate to inform the EDPS. The EDPS response to such data breaches will obviously depend on a number of factors including the seriousness of the breach, the type and volume of data involved, the numbers of data subjects affected, the location of the recipients, etc.

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

79 When personal data is processed via a mobile device, the user might store copies of personal data from central information systems on the device. This 'secondary storing' may lead to problems regarding the quality of the data, exercise of the rights to rectification, blocking and erasure by the data subject and as for the respect of the relevant data retention period. It might be the case that these data stored on the mobile device are not accurate or kept up-to-date, whereas the data are updated in the central storage system of the EU institution. The risks for the EU institution are increased by this possible lack of awareness of the processing operations taking place via a mobile device.

For example, a staff member of the HR department of an EU institution downloads on the mobile devise the document attached to an e-mail containing the personal data of a colleague.

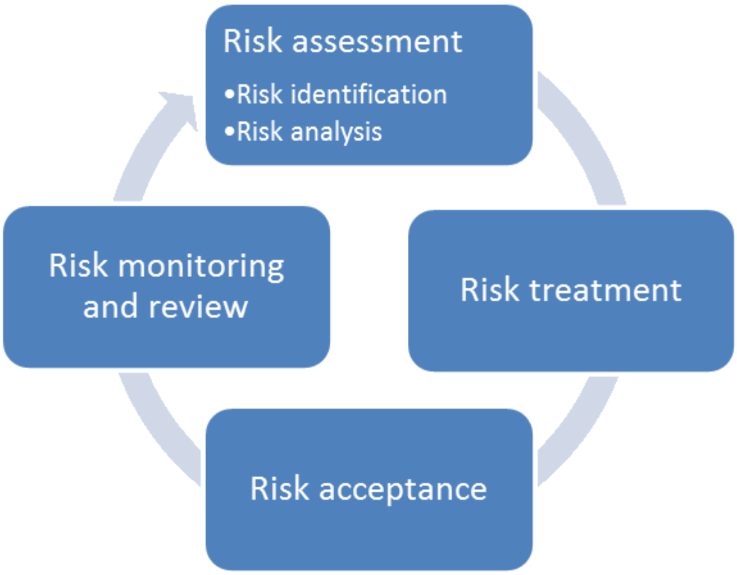
Under another possible scenario the user may use an application that replicates in the cloud the information stored in the mobile device without user's awareness. This scenario presents further risks regarding the confidentiality of the personal data being processed.

80 In case local copies of personal data on mobile devices are part of the processing operation as designed by the EU institution, it is also essential that when the data subject exercises the right to rectify the personal data that are inaccurate or incomplete or the right to block or erase unlawfully processed data, the personal data stored on the mobile device are also considered for rectification, blocking or erasure.

VI. Risks for personal data processed by mobile devices

81 This section provides a list of typical risks and threats to personal data in mobile devices, which should be considered by the EU institutions when performing their own risk assessment. This list provides a basis for identifying the most important risks and threats although it is not exhaustive: The actual risks and the security measures to control those risks need to be determined by each EU institution in the context of their assessment.

As a reminder, in the next diagram the main components of the risk management process are presented.



82 Mobile devices present more risks to personal data than desktop computers due to their portability, and, in case of smartphones and tablets, their ability to collect and share large quantities of contextual information, their 'always-on' nature, their number and diversity of sensors[17], and the users' expectation of a 'seamless interaction'.

83 Mixed use of mobile devices both for private and professional purposes may bring a further layer of complexity. Personal data processed in the context of professional life could potentially be processed without authorisation and its confidentiality, integrity and availability compromised while using the device for private purposes and vice-versa, even without the knowledge of the user.

84 The most relevant **risks** to the personal data are:

- accidental loss of personal data;
- alteration or destruction of personal data due to an unlawful access to users' personal data by mobile devices administrators, including remote switch off and remote alteration/wiping of personal data (photos, videos, local contacts, local copies of e-mails, documents, etc.);
- leakage of personal data due to non-authorized access to those data possibly also causing reputational or financial damages to the EU institution;
- unlawful geographical location of the user by potential attackers via location services;
- identity theft through the compromise of credentials (usernames, passwords, certificates) stored on mobile devices.

[17] For instance: GPS, digital compass, gyroscope, accelerometer, ambient light sensor or environmental sensors capable of measuring atmosphere pressure, temperature and humidity.

85 The most relevant **threats** that could lead to the previous risks are:

- mobile applications and/or the mobile devices unlawfully collecting and processing personal data;

> *E.g.: geographical location of the users without their consent. Analysing text messages exchange for commercial profiling.*

- customisation by device manufacturers, carriers and OS developers leading to locked configurations and features;

> *For example, not being able to deactivate location (GPS) sensors or to limit what information the mobile device sends to the vendor of the device or the provider of a particular application.*

- intentional exploitation by hackers (externals or insiders) of mobile devices vulnerabilities to target personal data (directly o as a side effect of the targeting of business related data);

> *E.g.: an infected PDF file is sent to the user of a mobile device with the aim of compromising the device to be able to read the user's emails.*

- accidental loss or theft of the mobile device;
- tampering physically with the device for accessing the information in it or for installing malware;

> *The mobile device is left unattended in a hotel or meeting room and because of that somebody physically interacts with the device and manages to install/modify the applications contained in the mobile device or to physically alter the mobile device itself.*

- misuse;

> *Due to a wrong configuration the user is able to disable the firewall installed on the mobile device. For using a specific application the user disables the firewall even if the user is aware that it is forbidden by the organisation policy.*

- human error.

> *The user ignores a security warning provided by a mobile device and the device is infected with malware.*

VI.1. Breach of the stored data

86 If adequate measures to secure the data stored on the mobile devices from unauthorized or inappropriate access are not in place, the EU institution may be exposed to potential financial, reputational, or even physical harm.

> *Some examples may illustrate this threat:*
> *• a mobile device is stolen, including the personal data stored thereon;*
> *• a mobile or storage device is disposed of into the trash or sold without removing the personal data so that the person who acquires the device may have access to the stored personal data;*

• institutional/private information stored on the device may be exposed to applications used for private/professional purposes;
• file sharing and file storage applications may make confidential information available to third parties;
• personal data is stored in the cloud and then compromised.

VI.2. Processing of 'third party personal data'

87 Some of the personal data processed through mobile devices relate to individuals which are not staff members of the EU institutions: *third party personal data*.

For example, a user from an EU institution may access an institutional application containing personal data and download these data into the mobile device. This new "database" ("shadow database") contains the same personal data as the "original" institutional application but would not be protected by the security measures in place for the latter (e.g. access controls by strong authentication measures) or in case of download on the EU institutions' personal computer (traditional hardware).

88 If we consider that mobile devices are subject to higher risks of loss or theft, and that the security measures which can be implemented on a mobile device are limited, it is evident that the data protection risks are considerably higher in this scenario than in case of normal access to the institutional database by personal computers.

VI.3. Interception of communications

89 Interception of communications may be defined as the observation or monitoring of an individual's communications or activities. Monitoring someone's activities typically happens in three ways: by eavesdropping on their communication; by inspecting data that is collected by communication activities (metadata); and by gaining access to the mobile device itself.

Examples of factors and means used for interception of communications include:

• lack of security in communication protocols to protect e-mail or web traffic;
• malware on devices;
• privacy invasive applications that access and use personal data in illegitimate ways.

For example, a compromised WiFi public access point may be used to perform a man-in-the-middle attack and extract information from the communication of the users.

VI.4. BYOD specific risks

90 The possibility for EU institutions' staff to use ("bring") their own mobile devices for accessing institutional information may bring some benefits to both EU institutions and their staff. Nonetheless, this also comes with added risks. The degree of control that the EU institutions and their IT departments can exercise -also having regard to the configuration of the devices- might be reduced in the BYOD scenario as compared to a scenario where the devices and the apps are preselected, approved and managed by the EU institution.

91 If the mobile device connects to the network of the EU institution it may present an additional risk (also due to the unfeasibility of managing the security of the mobile device). Rogue applications and malware may use the personal device for intruding into a protected network.

92 As remarked, BYOD leads to blurring of personal and professional use. The EU institutions risk getting access to personal and private data of their staff members (e.g. by accessing personal data synchronized to the institutional infrastructure), and the staff members risk exposing institutional information through the use of personal services like cloud storage or backup (easily activated by the users themselves), or via applications installed for personal uses which could subsequently offer 'gateways' for unlawful access to information hold by the EU institution.

93 The wide offer on the market of different models of mobile devices using different operating systems makes it difficult if not impossible for the IT departments of the EU institutions to provide support regarding the choice and management of all these devices. In addition, the IT department will hardly have any control on security updates and configurations which may be applied by the user or by the mobile device provider. None the less, the complexity and difficulty, under both a legal and a technical point of view, of the data protection aspects of the data processing by EU institutions by an IT infrastructure making use of mobile devices provided to staff members, cannot be used by EU institutions as a justification in case of lack of compliance with the Regulation. Ultimately, if the data processing entails processing of particularly sensitive data and information, a 'not-to-go' decision could be envisaged by the EU institution, not allowing for example the use of mobile devices (either institutional-owned and/or under the BYOD scenario) for the collection, storage and transmission of these personal data.