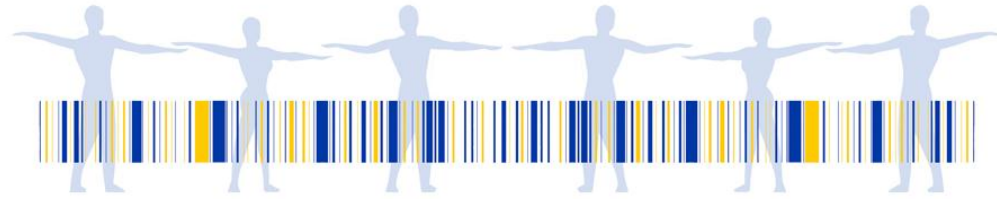




EUROPEAN DATA
PROTECTION SUPERVISOR



Mobile devices workshop

19/09/2013

Strategy

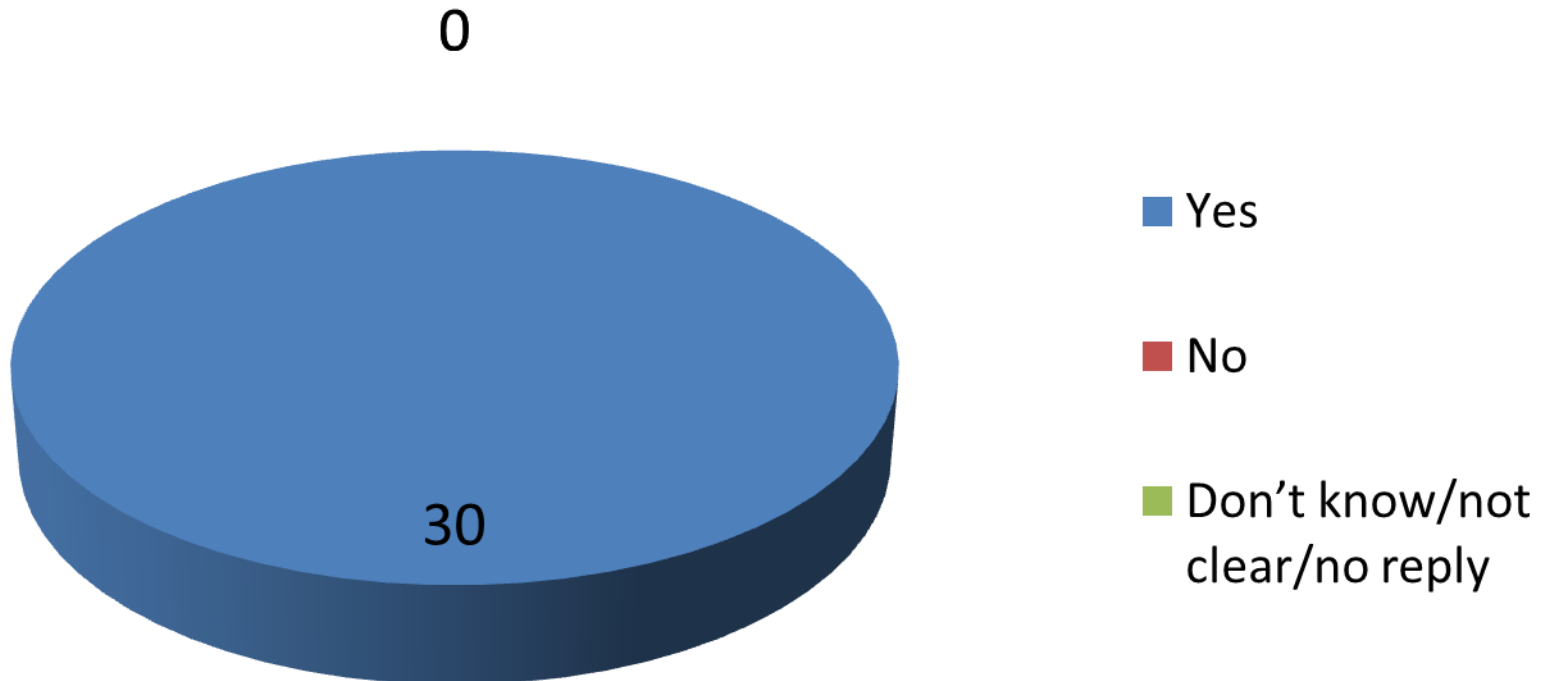
2013-2014



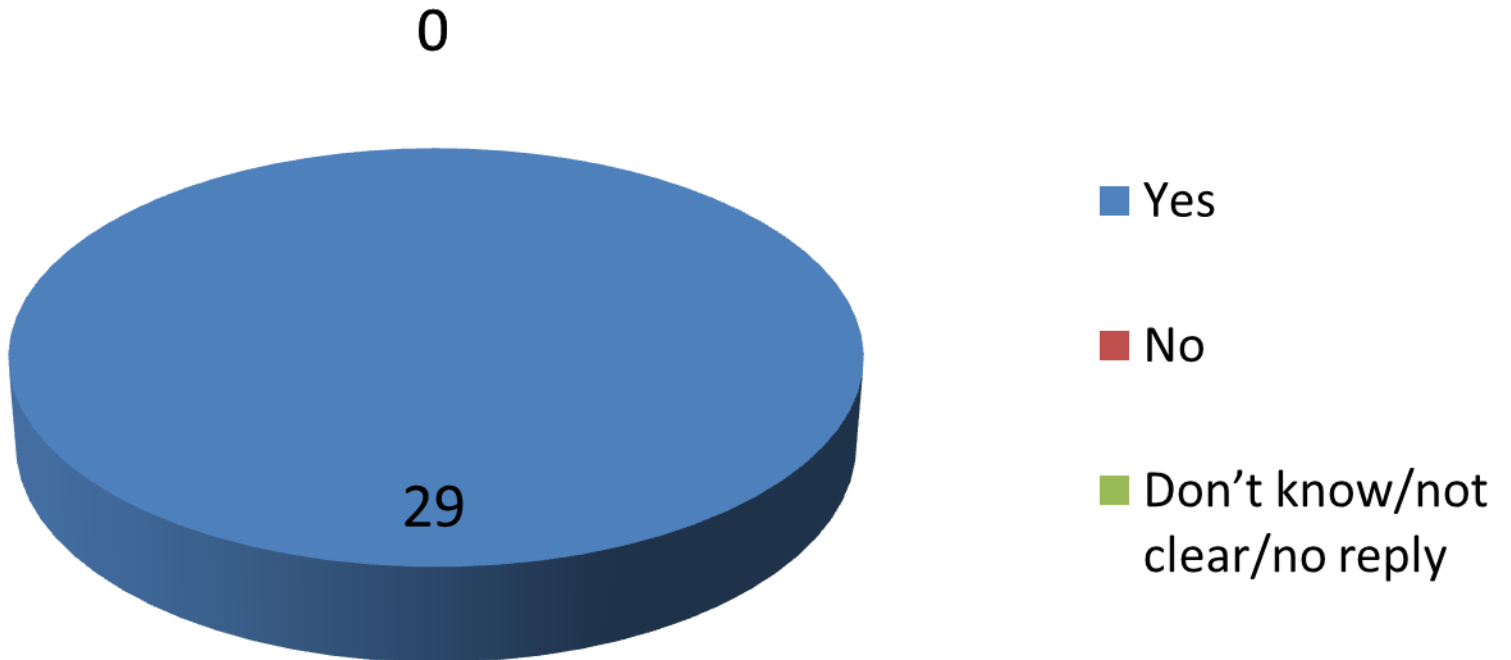
14.45 – 15.00

Results of the mobile devices survey

Do you use mobile devices for professional purposes ?



Do you provide staff with corporate devices?



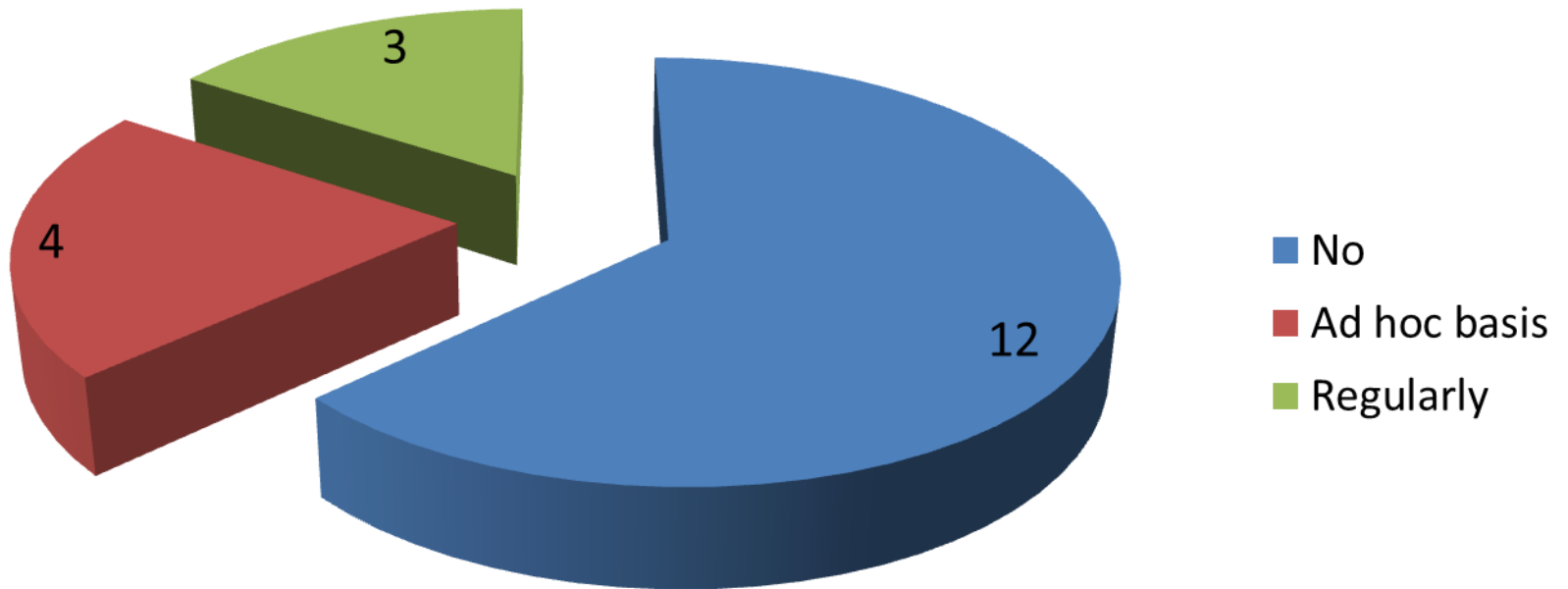
Risk Management

- **How do you manage the risks to personal data linked to the use of mobile devices?**
- Some conduct a risk assessment that includes the use of portable storage devices.
- Others are planning it.
- Many have policies they apply on devices which take into account specific risks (e.g. loss and increased risk of theft) without an assessment.
- When an assessment is carried out, though, mostly security risks are considered

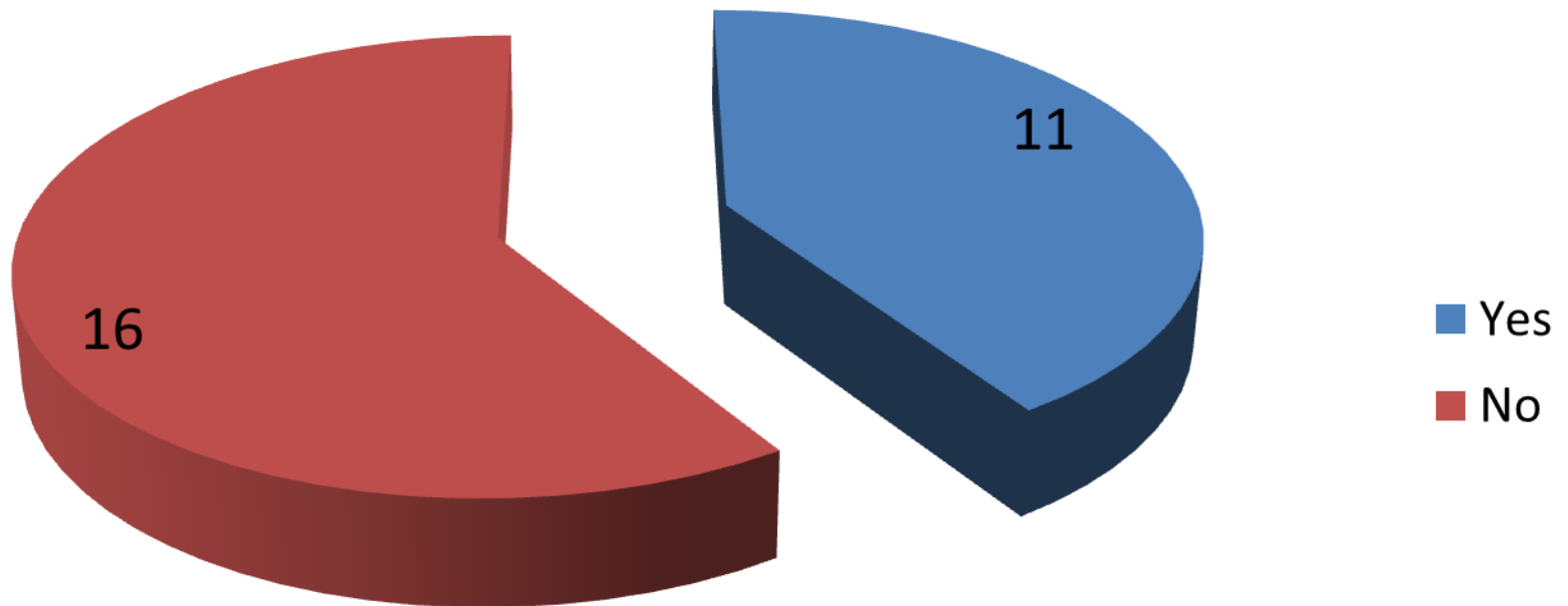
Typical countermeasures:

- Device encryption (mostly for laptops);
- Password policy
- Inactivity lock
- Anti-malware
- remote full device wiping in case of theft or loss
- encrypted connection
- Blocking change of device settings and app installation
- limited access to applications/information
- secure apps
- minimising the amount and the sensitivity of the data on the device.

Is the DPO involved in risk management?



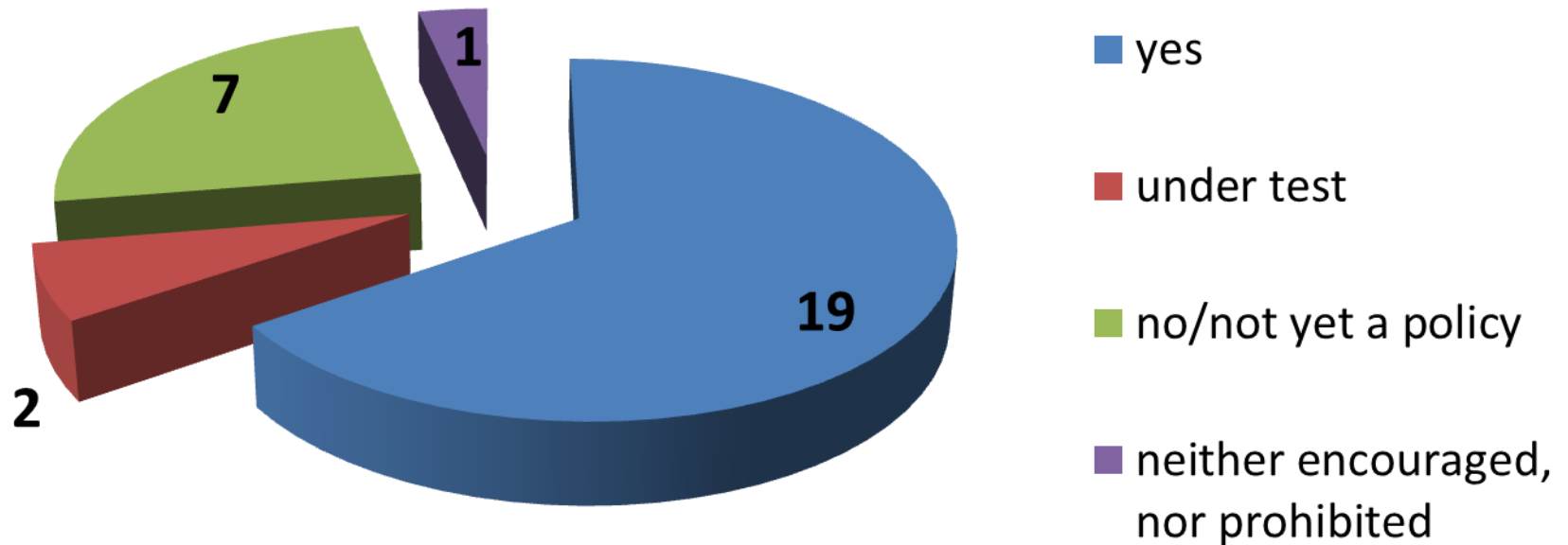
Do you have any specific policies for the use of mobile storage devices ?



Technology used

- What devices do you use (type, brands, models) and what is the software (OSs, specific SW, apps etc.) available on your communication mobile devices:
 - Most corporate smart mobile devices are either Iphones (iOS) or Blackberries, with a few Window mobile and Symbian based devices. Among supported OSs Android and all the above are supported. Some provide management with Ipads (iOS),
- Do your mobile devices have brands' and carriers' customisation?
 - The replies show some misunderstanding. Overall half of the replies report OSs and carriers' customisation. None seems to have devices coming with a configuration required by the institution/agency
 - On the other hand, most of the institutions configure corporate devices according to their policies

Do you allow the use of private mobile devices for professional purposes (BYOD)?



15.00 – 15.15

Personal data processed in mobile devices and associated risks

- Professional purposes. Mixed use for private and professional purposes
- Personal information of the device's users, their contacts and other people.
- Risks to privacy and other fundamental rights: confidentiality, integrity and availability
- Legal rules
 - Article 36 of the Regulation
 - Directive 2002/58/EC

15.15 – 15.45

Accountability, data protection Management and principles

- Data controller responsibility/DPO roles
- Mobile devices configuration and operation in light of data protection requirements
- Awareness of data protection principles.
- Data protection risk assessment
- Privacy by design and by default
- Comprehensive information

15.45 – 16.15

Mobile device management

- Risk assessment: Corporate owned devices/BYOD schema/Mixed approach
- Mobile Device/Application Management systems
- Data minimisation and purpose limitation
- How do you document processes, define roles and responsibility
- Data protection requirements taken into account in the policy
- Information to data subjects
- Countermeasures with respect to legitimate expectations

16.15 – 16.45

Mobile device security

- Security risk management process & policies
- Allocation of responsibilities
- User awareness training
- BYOD policies and special requirements in terms of security
- Privacy-friendly default configuration of mobile devices and applications
- Management of security incidents
- Information of users on breaches

Process towards Guidelines (websites and mobile devices)

- **Survey**
 - Start collecting facts and understanding institutions reality
- **Workshop**
 - Orientation document for further insight and first perspectives
 - Other exchange opportunities as requested (IT managers, webmasters etc.)
- **Draft guidelines** (tentatively Oct 2013)
 - Your feedback on draft guidelines (tentatively Nov 2013)
 - Final consultation (?)
- **Guidelines**