Cloud Security Alliance Italy Chapter

BYOD: a next step forward for the IT revolution started with Cloud

Considerations from the point of view of data protection & monitoring of workers

November 2013

Document Sponsors

Foreword

The new study launched in the year 2013 by CSA Italy Chapter in corporation with New Zealand Chapter, brings data protection & privacy as well as monitoring of workers perspective to the theme "Bring Your Own Device" (BYOD).
For the purpose of this study, BYOD means tablets, smartphones, portable and mobile terminals that access data and applications remotely for business purposes of an employer.

The study aims to highlight the importance of these regulations and one of the its purposes is the set up of a summary table considering the references of applicable legislations in the contexts of some EU/not EU countries, hopefully to be enriched and kept up to date with further contributes from CSA volunteers.

The other essential purposes of the study is the proposition of a framework of key measures for BYOD at work (the so called Golden Rules) and of a systematic process "BYOD Impact Analysis" for the introduction of BYOD applications in the work organizations, with special reference to the requirements coming from the laws

Valuable input for the study has been represented by the resources drawn up by CSA Global about the Mobile Computing:

Security Guidance for Critical Areas of Mobile Computing[1]

Mobile Top Threats[2]

Mobile Device Management: Key Components[3]

[1] https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-mobile-computing/

[2] https://cloudsecurityalliance.org/download/mobile-top-threats/

[3] https://cloudsecurityalliance.org/download/mobile-device-management-key-components/

Table of o content

Acknowledgements

Coordinator of the Working Group "Legal & Privacy in the Cloud"

Valerio Vertua

Contributors

Gloria Marcoccio (Team Leader)

Rizwan Ahmad (Cloud Security Alliance New Zealand Chapter)

Ettore Corsini

Martina Lindblad

Valentina Malandrino

Thanks to Rasmus Rosenqvist Petersen, Founder of NOBLACKBOX Cambridge Ltd., for his contribution regarding the BSI Guide on Privacy Impact Analysis

CSA Italy Staff

Matteo Cavallini (Coordinatore Comitato Scientifico)

Review

Comitato Direttivo

Comitato Scientifico

Document Sponsor

Trend Micro

Itway

1.0 Introduction

Operation and maintenance of IT infrastructure with logistic and support concerned, is surely one of the essential enabling factors for business and represent an unavoidable important cost element for the companies, whatever their dimension.

Cloud computing has given a first strong jolt to this state of IT affairs, opening to new approaches in delivering and using IT services , changing maybe forever the way the companies are managing IT matters.

Now a new source of huge modifications for how the companies face IT is already active and likely to produce in the next future upheaval at several levels within the organizations: the BYOD - Bring Your Own Device - revolution.

Rather than the company provides to workforce electronic devices (smart phone, tablet, laptop), the company allows the worker to use (brings to work) his/her personal electronic devices. In a BYOD work context, the company provides the hardware and storage for the information and the worker provides the devices through which that information is accessed and used for company business purposes. The workers use their personal electronic devices for two concomitant reasons: for their own personal purposes and for company's need.

This approach has important impacts on the company IT management system made of people and devices requiring consistent amount of human and financial resources, on security and liability in front of the law for the use of BYOD in the twofold environment "business & personal" and definitely dictate for a sound review of the company policies concerning IT, security and ethic behaviour, bearing in mind that, for many reasons, still it could remain in place the use of portable devices provided by the companies.

BYOD is certainly a complex and new matter which poses a number of questions from many points of view: in this study we decided to propose some analysis, open to discussion and further investigations, from the perspective of regulations related with privacy & personal data protection and monitoring of workers affecting the BYOD company internal regulations.

2.0 New issues

BYOD is a recent topic, therefore each of us can pose many questions considering his/her experience and knowledge of the matter.

We do not yet have all the answers, however the scenarios that could trigger advantages for all the parties interested as well as involve area of concerns and needs for proper solutions, should in our understanding include the following considerations

- From the company information security perspective, BYOD devices must be configured and managed with controls commensurate with the sensitivity of the underlying data as part of an overall and new risk management framework

- Following the trend of consumerization[4] of Information Technology, the companies meet and take advantage of the personal preferences of workers, offering them increased mobility and better integration of their personal and work lives

- BYOD enables workers the flexibility to work in a way that optimizes their productivity

- BYOD dictates for a deep company cost-benefit analysis, taking into account both potential increases in worker productivity and potential cost shifts. Providing workers access to company information systems and services on their personal devices should help reduce the number of portable devices that are provided to the personnel as well as the associated life-cycle in terms of asset management and costs. BYOD may, however, involve the implementation of company reimbursement procedures for voice/data costs incurred when workers use their personal devices for business and additional infrastructure costs in handling the support of BYOD users

- Implementation of a BYOD program presents several security, policy, technical, and legal challenges not only for company internal aspects but also to relationships and trust with Customers and Partners.

- Who owns the phone number/communication enabler? On their personal devices, workers could make many calls to company's Customers or for accessing the company business services necessary to perform their work activities. The worker could leave the company, but Customers continue to call the individual, former company's worker. What about the rights of the company on the former worker's phone number: any negotiation or statement before the workers leave could represent a viable solution

- Does checking e-mail count as overtime? This could represent an already hot-topic in employment law in several countries BYOD grant hourly workers a great freedom to check e-mails outside of normal working hours, and employers should pay attention on such activities can violate laws regarding wage or hour account

[4] http://consumerization.trendmicro.com/consumerization-trends-for-2013/

- Should the company remote wipe a personal device? The employer could remotely wipe the personal device that the workers had been used, for example, before leaving. In doing so, the employer also could inadvertently disrupt in such a way the individual's personal data. How to manage liabilities in this regard?

- E-discovery and data retention on BYOD. The ever-expanding realm of e-discovery would most certainly include personal devices used in BYOD work context. What about the rules to apply in order to preserve and collect the information stored on the personal devices.

- And more …

3.0 Why considering privacy and work-monitoring laws

The BYOD usage in the twofold context “personal&business” of BYOD workplace involves several types of activities made both by the individual and by the employer organization that can be summarized as shown in the following figure.

Fig. 1 - Summary of main BYOD uses in the context of BYOD workplace

Here below we report some examples about typical data & processing made with regard to the BYOD context:

- Personal use of the device made by the worker (for calling, purchasing, viewing information, receiving personal call,…)

- Technical control of the device operated by the employer for the purpose of:
  - granting access to companies business facilities and services
  - operation & maintenance of the company software agents and hardware component loaded in the BYOD for business purpose
  - for assessing fulfillment of company ethic/security/technological… policy
  - for the need arising from any kind of litigation or complaints
  - for assessing the proper performing of the activities in charge to the worker
  - for managing the company workforce in terms of allocation of tasks and activities (real time localization of workers,…)
  - ……

- Personal data stored/processed along the worker personal use of the device

- Personal and business sensitive data for which the employer is responsible (as data Controller, as Data Processor) made by the worker via the device used for business purpose

Therefore the implementation of a BYOD program definitely requires the companies to pay the upmost attention for balancing their own security and confidentiality purposes with the privacy and data protection rights of the workers as well as for fulfilling the national laws applicable in the context of monitoring of workers.

4.0 Golden rules

Allowing the use of personal mobile devices at work will help the organizations achieve agility in conducting their business and improve workers' morale & commitment by putting a BYOD policy in place.

However this process requires appropriate control and governance in the company since the advantages could turn soon in risks for the business, bearing in mind that BYOD modifies the information security context with new threats and vulnerabilities and requires a clear legal ground in terms of compliance with the applicable laws, *in primis* concerning data protection, privacy and monitoring of worker.

The twofold context "business & personal" is made up of new practical use cases that we still cannot know fully and in detail to the extent necessary for identifying a detailed framework of BYOD controls, also considering the extreme variety of platforms and technologies that BYOD involves.
However, considering the scenario of new BYOD issues we tried to lay down in Chapter 2 and taking into account the typical requirements brought by the laws in subject, the authors of this study have represented with the following 10 golden rules (briefly reported in the following para.) the essential elements proposed as pillars for building a robust BYOD governance & related framework of controls.

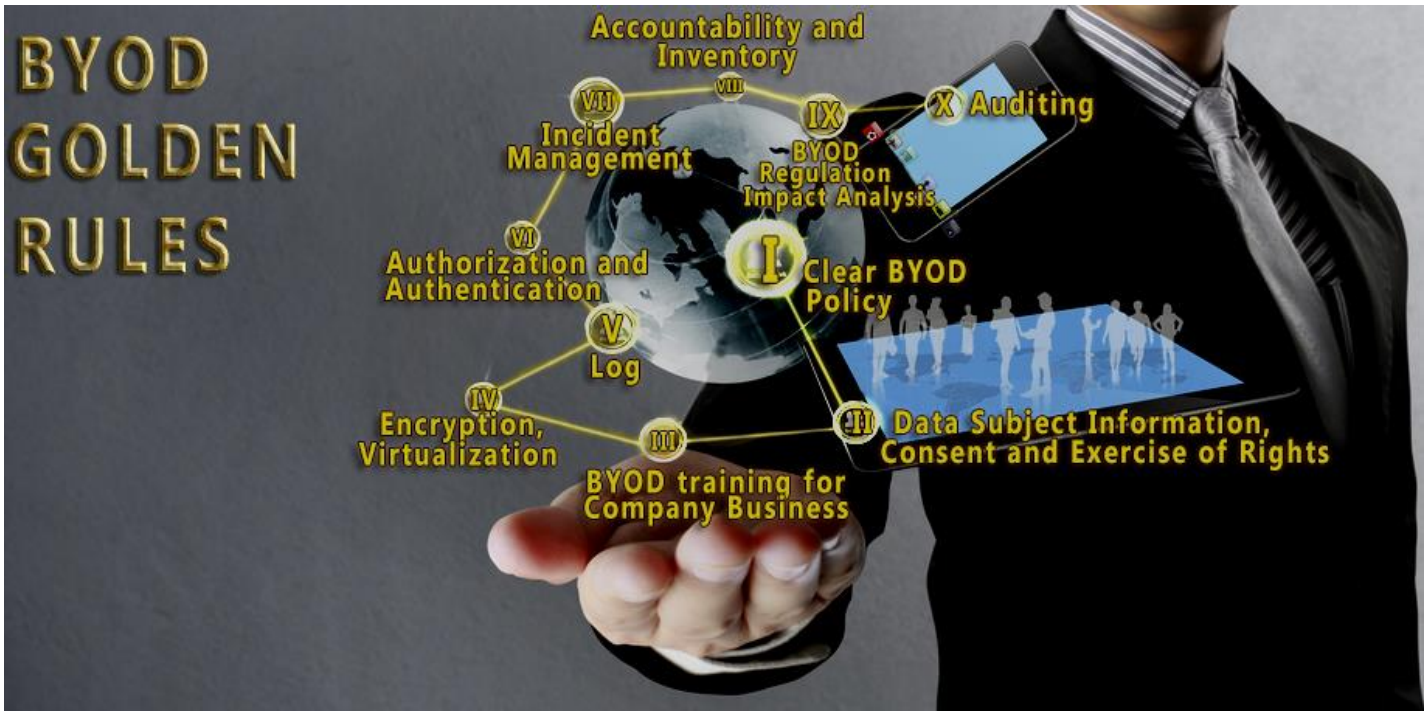


Fig. 2 - Golden rules for BYOD in workplace

4.1 Clear BYOD policy

The BYOD usage in the workplace involves for the user new freedoms and at the same time new constraints , both with complex legal implications, therefore a clear policy in BYOD usage is certainly

the measure number one that the organizations have to carefully prepare, implement, communicate and keep updated.

A not exhaustive list of BYOD policy rules should include:

- A clear explanation of what the policy is and its scope
- A financial disclaimer and/or explanation in order to clarify whether the employer has some responsibility in contributing to the purchasing of the mobile devices and related replacement/maintenance aspects
- Credential controls for the use of BYOD for business purpose, such as user-account & password requirement. For example a control could be: settings of password or PIN code should be so that a password/PIN prompt appears after N minute of inactivity, when the device is powered on, or when the device is woken up
- A privacy disclaimer. The BYOD policy should make clear how is ruled the privacy rights in the device(s) used
- A liability disclaimer. The employer should clarify any liability or responsibility for damage to, or the loss/corruption of data stored on, a device used as part of the BYOD policy
- A search/access agreement. The BYOD policy should make clear which rights has the employer to physically and remotely access any device used as part of the BYOD policy
- A limitation on access/use. Rules about if and how and according to what terms the third-parties (sons? friends?...)should be allowed to use and/or access any device used as part of the BYOD policy
- An incident reporting requirement. The BYOD policy should require workers to immediately report to the employer any incident (including events such as lost or stolen devices) occurred to the device under BYOD policy
- A written BYOD policy acknowledgment. All BYOD workers should acknowledge in writing that they received the policy, understand it, and agree to be bound by it.

4.2 Information-Consent exercise of rights

According to the applicable data protection & privacy law the employers shall implement their BYOD programs bearing in mind that the workers is a “data subject” for the processing the employers made in their role of data Controller (example: geo-localization of worker for business purpose), therefore prior Information to the worker, his/her consent acquisition when required by the law and the respect of his/her privacy rights (such as access his/her data) are part of the enabling factors for a lawful use of BYOD devices by the employers.

4.3 Training on BYOD usage for business purpose

A robust implementation of any BYOD policy certainly takes advantages from the definition of BYOD communication plans and specific training courses in order to allow the worker to effectively be able to use the BYOD for business purpose.

4.4 Encryption

Although there are already on the market a number of applications able to create internal barriers on personal devices, preventing the mixture of company and personal data, encryption functionality still represents one of the best effective security measures for protecting company data accessed/stored in a BYOD device.

Furthermore, encryption can be considered an essential natural separator between the different liabilities of employer and worker when using the BYOD , each one for his purposes.

4.5 Log

Log of accesses to company information systems and resources accessed via BYOD is a typical security measure able to support a variety of security controls and also to serve as a basis for forensic investigations in case of breach of company policies or of criminal actions conducted using worker mobile devices.

4.6 Authorization/Authentication process

Authorization and authentication process are well known and used measures to protect and control access to company data and data processing. They need to be properly assessed from the BYOD perspective in order to be able to perform properly also in the BYOD operative context.

4.7 Incident management process

Incident caused, intentionally or not, with BYOD, are a matter for many to new, however it is not difficult to predict that their number and ability to cause severe damages in the organizations is expected to grow in the short term. Therefore any company incident management process shall carefully spend appropriate effort and resources to assess the specific company threat-vulnerability context for BYOD and identify remediation measures. This topic should be at the utmost attention for the company since data breaches laws are already in place in some sectors (as it is the case of publicly accessible electronic communication services in the European Union) and new incoming laws are expected to spread in whatever business sector (next new EU privacy regulation[5], which is intended to replace the eighteen-old data protection directive 95/46/EC.)

[5] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

4.8 Accountability

BYOD for business usage operatively maps in to activities that can be done and data that can be accessed by the worker and by the employer: for liability segmentation and for making the employer able to effectively operate the BYOD for its part of responsibility, it is essential to implement the accountability principle:

In IT context: to establish what is done by which mean and for what reason (involving as a consequence also hw and sw configuration management processes)

In law context: the ability to demonstrate that appropriate measures have been taken for the purpose of law compliance

4.9 BYOD Impact Analysis

The implementation of any BYOD related business capability or service requires a structured and systematic analysis of the legal implications related to intended new functionalities. For the purpose of this study, the legal implications are here limited to the privacy and worker monitoring laws: a specific approach is proposed in chapter "BIA: Guidelines for BYOD Impact Assessment".

4.10 Audit

Governance of any control system, whatever is the context or areas concerned, always implies an audit process. In the BYOD context the audit gains a further importance considering the legal implication of BYOD usage and therefore the necessity to periodically assess company compliance status in this regard.

5.0 Catalog of privacy and work-monitoring laws

The trend fuelled by the expected consistent IT costs reductions, imposes the companies to realize that BYOD is happening, regardless it is officially sanctioned or not, and to take steps to implement organizational/procedural/technology solutions that secure company's data across a range of different BYOD platforms and devices.

One important aspect of coping with BYOD is the impact deriving from workers data protection legislation and how this creates constraints for organizations in implementing a BYOD policy. For example, operating a mobile device management solution on a personally owned device will, in most cases, entail a certain degree of activity monitoring and access to data. This can involve for the organization the risk of breaching the workers' data privacy rights and therefore open to a lawsuit. Furthermore, breach of law with regard of the monitoring of worker is likely to be a risk most real.

Companies have therefore to face and balance two opposite objectives: they must protect business data accessed on a worker-owned device, with specific regard to customer data and business critical data, as they will be liable in the event of data loss or misuse, but they must do so without breaching the applicable national laws ensuring protection for workers in terms of their privacy and rights concerning monitoring at work.

Therefore the awareness of the essential applicable laws in terms of privacy & data protection and workers monitoring became a must for an effective implementation of companies lawful BYOD programs: the requirements brought by these laws should be processed with high priority in any BYOD implementation plan before to set up investment plan for the necessary hw&sw operations and IT personnel concerned.

In the above mentioned "Golden rule" no 9, the BYOD Impact Assessment, these law represent the essential input to be identified, assessed and processed as a "risk" to be mitigated.

For the purpose of this study, it has been activated a collection of the relevant privacy and work monitoring concerned laws, modeled according to the following schema.

BYOD LAWS CONCERNED – EXECUTIVE SUMMARY - Schema

Nation of the Law *(if EU legislation write: EU)*
Number of the Law
Title of the Law
Type of law *(Decision, Regulation, Law, Legislative Decree, Order of Authority, ….)*
Date of issue of the Law
Hyperlink to official source where to find full text of the law *(no commercial website!)*
Sector of the Law (chose one of the following: **1) Work law** **2) Privacy law** **3) Other)**
Is it a national law transposed from an EU Law? *According to the case write: Y or N. In case Y please report the Number the Title the Type the Year of issue of the EU Law concerned*
Executive summary of the law requirement *Briefly describe what is the requirement*
BYOD impacts *Briefly describe why the requirement has impacts on BYOD*
Does the requirement impose organizational/procedural measures to the employer ? (example: provide information, prepare a company policy,…) *According to the case write: Y or N. In case Y briefly describe the required measure*
Does the requirement impose to the employer communication/agreement with Unions and/or related Government Offices? *According to the case write: Y or N. In case Y briefly describe the required measure*
Does the requirement impose to the employer communication/agreement with competent Authorities? (example: Data Protection Authority) *According to the case write: Y or N. In case Y briefly describe the required measure*
Does the requirement impose technical measures? *According to the case write: Y or N. In case Y briefly describe the required measure*
Does the requirement impose behavioural measures to the employee? *According to the case write: Y or N. In case Y briefly describe the required measure*
Sanctions *Please briefly describe, if any, the sanctions established by the Law (and refer the related Article)*

The actual content of the BYOD LAWS CONCERNED – EXECUTIVE SUMMARY is reported in Appendix 2

Volunteers of CSA are encouraged to give their contribute for the law countries of their knowledge, the contact point for this initiative: Team Leader of this study.

6.0 BIA: Guidelines for BYOD Impact Assessment

This guideline has been designed bearing in mind that the implementation of any BYOD related capability or service requires a structured and systematic analysis of legal implications related to functional requirements (organizational/technical/procedural), with regard to privacy and worker monitoring for the scope of this study.

The approach followed is based on the Privacy Impact Assessment in the RFID context, as depicted formerly by the WP 29 with its works and opinions and then very recently by BSI with its RFID PIA Guide (See para "BIA References" below)

6.1 Purpose

An employer (organization) who is in the progress of allowing the use of BYOD for business purposes by the employees/external collaborators (workers) has to take into account measures and allocation of responsibility for:

1. protecting its business information accessible by means of BYOD
2. for its part of liability, protecting privacy and confidentiality of personal information that can be accessed/processed by means of BYOD
3. operating its organizational/administrative measures necessary for the coordination of its business activities, considering the specific characteristic of BYOD (portable device closely connected with the individual who brings it)

6.2 BIA objectives

BIA is intended to be a process, based on a risk management approach, with the aim of supporting the systematic fulfillment of privacy & data protection law requirements as well as worker monitoring law in the employer-workers relationships.

The essential source of these requirements is represented by the applicable privacy and data protection laws and regulations and the legislation about the possible monitoring on the worker.

Similar approaches have been already analyzed and documented with the works of relevant bodies such as:

- In Europe: UK Privacy Commissioner's office (see para "BIA References" [1])
- In United States of America: U.S. Department of Homeland Security (DHS) (See para "BIA References" [2])

These works focus on the so called Privacy Impact Assessment (PIA).

An important customization (see para "BIA References" [3]) of the PIA process for RFID applications has been prepared by RFID industry representatives and endorsed by WP 29[6] and, very recently, BSI with the UK Department for Business Innovation & Skills issued a specific implementation guide always for the RFID scope (see para "BIA References" [4]).

Extending the PIA approach to BYOD purposes, the expected results for a BIA should be:

- the identification of the privacy & data protection impacts;
- the identification of the impacts from the laws concerning the workers monitoring
- the identification of the Organization's requirements for protecting its business information accessible by BYOD
- the provision of the basis for awareness of the impacts for all the stakeholders having liability in front of the law (Organization as Employer, employees/external collaborators, third Parties providing service on BYOD,…);
- document the results of the assessment, to be used for:
    - BYOD policy preparation/up date
    - accountability purposes
    - provide input to necessary implementations

[6] This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

6.3 Essential BIA flow

The proposed BIA process starts with a first phase of analysis by which to determine whether an effective BYOD Impact Assessment is required, and then, in case of positive result, a second phase follows, to perform the risk analysis, identification of the measures and their documentation.

First phase is here called BTA: BYOD Threshold Analysis, second phase is the effective BIA: BYOD Impact Analysis.

In the following the term "service" denotes the function/capability to be analysed for BIA purposes.

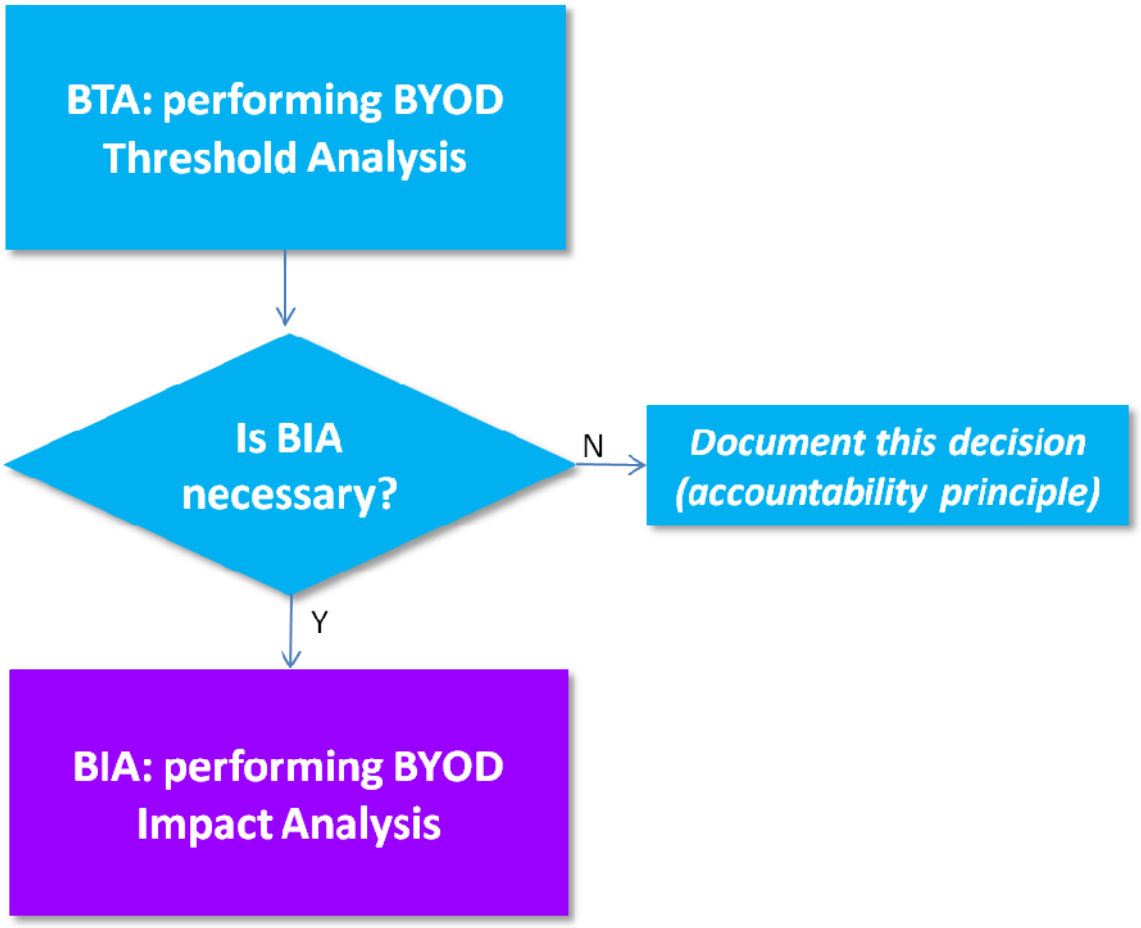


Fig. 3 – Essential BYOD flow

6.4 BTA phase

The tasks of this phase are:

1 Identify the national applicable laws

according to the specific service and its context of use (target users, establishment of service provision centers,..) one or more nations could be the sources of applicable laws

2 Applicable law

2.1 Verify whether the service processes information subject to the data protection and privacy laws of the applicable national laws identified in step 1

2.2 Verify whether the service processes information subject to any law regarding monitoring of workers of the applicable national laws identified in step 1

As a result of this task the service should be described with a list of all the kind of personal data and "monitoring data" it processes and the references for the applicable national laws concerned (primary legislation, secondary legislations, national competent authority's orders and decisions…)

3 Document the results – The output of BTA should be documented with an official report, since the BTA results strongly influence performances, characteristics and costs of the service as well as the liability of the company in fulfilling the necessary requirements of the laws here considered.

6.5 BIA phase

The tasks of this phase are:

1 Identify the "severity privacy & monitoring profile" of the service: according to its nature and context of use (target users, technology,…) it should be required to perform a classification that addresses security measures more or less stringent (see as example the case of RFID applications in [4] where is to be decided for a Full Scale PIA or a Small Scale PIA).

2 Then **activate a risk assessment process**. Risk analysis and countermeasure/controls identification should be activated considering the framework:

- Privacy & monitoring targets (both in the business and in the personal context of use for BYOD)
- Related risks (both in the business and in the personal context of use for BYOD)
- If applicable a catalog of counter-measures/controls to mitigate the risks.

In paragraph" BIA Appendix" below are listed in separated tables the privacy targets according to the principles of two fundamental sources of privacy legislation (U.S. and UE).

Privacy and monitoring risks are strictly related with the laws and regulations identified in the BTA phase and with the nature and context of use for the service.

The essential steps and deliverables of this task of risk assessment are:

2.1. Agree on a formal description of the service, to be used in the risk analysis;

2.2. Identify and list how the service could threaten privacy and monitoring and then estimate the magnitude and likelihood of those risks;

2.3. Document repartition of responsibility for actions and liability in front of the law for the main classes of parties: the employer and the employees/external resources

2.4 Document technical/organizational/procedural controls to mitigate identified risks;

2.5. Document the program by which the BIA results will be implemented including if any BYOD policy review and related communications to all the parties concerned

2.6 Document who in the Organization will be responsible and how it will be assessed that the BIA measures are in place before the go live of the service

Step 2.1: Agreed formal description of the service

This formal description should give a comprehensive and full picture of the service, its environment and system boundaries, as necessary to conduct an effective BIA. Since the quality and reliability of risk analysis and countermeasures identification strongly depend on this service description, clear agreement on this point is essential.

Step 2.2: Identification of Risks

The goal is to identify conditions that may threaten or compromise personal data making reference to privacy targets and monitoring constraints. The risks are to be determined considering the detailed applicable laws as indentified during the BTA phase and any functional requirement of the service with impact on privacy, data protection and monitoring

Step 2.3: Document repartition of responsibility for actions and liability

Effective deployment of requirements and consequent implementation of measures are enabled by a clear repartition of roles and responsibility to take actions and liability according to the applicable law.

Step 2.4: Identification and Recommendation of Controls

In this step are analyzed the controls to minimize, mitigate or eliminate the identified risks.

Controls are either of a technical or nontechnical nature. Technical controls are incorporated into the service through architectural choices or technically enforceable policies, e.g. default settings, authentication mechanisms, and encryption methods. Nontechnical controls on the other hand are management and operational controls, e.g. operational procedures.

The identified risks and their associated risk levels should guide the decision on which of the identified controls are relevant and thus need to be implemented, considering also the costs constraints affecting the service design & implementation. The BIA documentation should explain how the controls relate to specific risks, and should elaborate on how this mitigation will result in an acceptable level of risk.

Step 2.4: Documentation of Resolution and Residual Risks

Once the risk assessment has been completed, the final resolution about the service should be documented in the BIA Report, along with any further remarks concerning risks, controls and residual risks.

Approval for service design should be issued once the BIA process has been completed with relevant risks identified and appropriately mitigated to assure no significant residual risks remain in order to meet the requirements of compliance, with appropriate internal reviews and approvals.

6.6 BIA References

[1] "Privacy Impact Assessment Handbook", version 2.0, by UK Information Commissioner's Office

[2] Privacy compliance process of U.S. Department of Homeland Security

[3] WP 29 Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications adopted on 11 February 2011

[4] PAS 94:2013 Implementing privacy impact assessment (PIA) frameworks in radio frequency identification (RFID) application . Guide – BSI and UK Department for Business Innovation & Skills – May 2013

6.7 BIA APPENDIX

FIPPS U.S. reference for Privacy Targets

The Fair Information Privacy Principles (FIPPs) are here below reported.

FIPPS Privacy Targets	Description
Transparency:	COMPANY should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
Individual Participation:	COMPANY should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. COMPANY should also provide mechanisms for appropriate access, correction, and redress regarding COMPANY's use of PII.
Purpose Specification:	COMPANY should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
Data Minimization:	COMPANY should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
Use Limitation:	COMPANY should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
Data Quality and Integrity:	COMPANY should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
Security:	COMPANY should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
Accountability and Auditing:	COMPANY should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

EU reference for Privacy Targets

EU Privacy targets are tuned on the EU privacy Directive 95/46/EC

EU Privacy Targets	Description
Safeguarding quality of personal data	Data avoidance and minimization, purpose specification and limitation, quality of data and transparency are the key targets that need to be ensured.
Legitimacy of processing personal data	Legitimacy of processing personal data must be ensured either by basing data processing on consent, contract, legal obligation, etc.
Legitimacy of processing sensitive personal data	Legitimacy of processing sensitive personal data must be ensured either by basing data processing on explicit consent, a special legal basis, etc.
Compliance with the data subject's right to be informed	It must be ensured that the data subject is informed about the collection of his data in a timely manner.
Compliance with the data subject's right of access to data, correct and erase data	It must be ensured that the data subject's wish to access, correct, erase and block his data is fulfilled in a timely manner.
Compliance with the data subject's right to object	It must be ensured that the data subject's data is no longer processed if he or she objects. Transparency of automated decisions vis-à-vis individuals must be ensured especially.
Safeguarding confidentiality and security of processing	Preventing unauthorized access, logging of data processing, network and transport security and preventing accidental loss of data are the key targets that need to be ensured.
Compliance with notification requirements	Notification about data processing, prior compliance checking and documentation are the key targets that need to be ensured.
Compliance with data retention requirements	Retention of data should be for the minimum period of time consistent with the purpose of the retention or other legal requirements

Privacy risks proposed for BYOD context (derived from para. “BIA References” [4])

Privacy Risk	Description and example
Unspecified and unlimited purpose	The purpose of data collection has not been specified and documented or more data is used than is required for the specific purpose
Collection exceeding purpose	Data is collected in an identifiable form that goes beyond the extent that has been specified in the purpose
Incomplete information or lack of transparency	The information provided to the data subject on the purpose and use of data is not complete, data processing is not made transparent, or information is not provided ina timely manner
Combination exceeding purpose	Personal data is combined to an extent that is not necessary to fulfil the specified purpose
Missing erasure policies or mechanisms	Data is retained longer than necessary to fulfil the specified purpose
Invalidation of explicit consent	Consent has been obtained under threat of disadvantage
Secret data collection	Some data is secretly recorded and thus unknown to the data subject
Inability to grant access	There is no way for the data subject to initiate a correction or erasure oh his/her data
Prevention of objections	There are no technical or operational means to allow complying with a data subject’s objection
A lack of transparency of automated individual decisions	Automated individual decisions based on personal aspects are used but the data subjects are not informed about the logic of the decision making
Insufficient access rights managements	Access rights are not revoked when they are no longer necessary
Insufficient authentication mechanism	A suspicious number of attempts to identify and authenticate are not prevented
Illegitimate data processing	Processing of personal data is not based on consent, a contract, legal obligation,..
Insufficient logging mechanism	The implemented logging mechanism is insufficient. It does not log administrative processes
Uncontrollable data gathering from BYOD	There is poor level of confidence in the ability to gather data only for the intended business purposes

7.0 Bibliography

Please note: the content of all the on line references listed here below has been used as available till November 30, 2013.

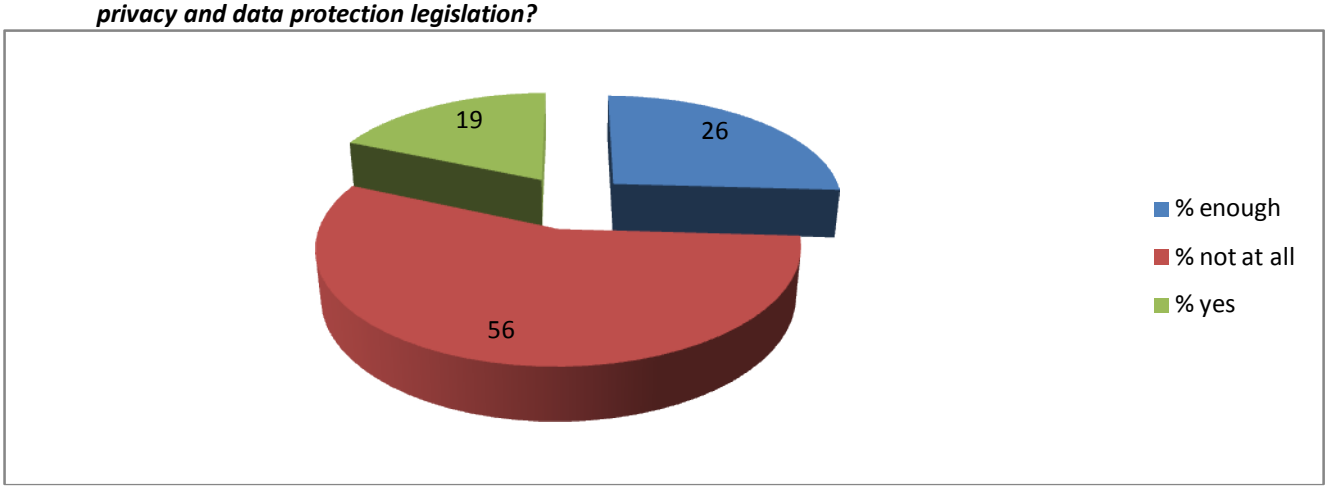
I.	**Security Guidance for Critical Areas of Mobile Computing** https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-mobile-computing/
II.	**Mobile Top Threats** https://cloudsecurityalliance.org/download/mobile-top-threats/
III.	**Mobile Device Management: Key Components** https://cloudsecurityalliance.org/download/mobile-device-management-key-components/
IV.	**Consumerization Trends for 2013** http://consumerization.trendmicro.com/consumerization-trends-for-2013/
V.	**"Privacy Impact Assessment Handbook", version 2.0, by UK Information Commissioner's Office** http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx
VI.	**Privacy compliance process of U.S. Department of Homeland Security** http://www.dhs.gov/files/publications/gc_1209396374339.shtm
VII.	**WP 29 Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications adopted on 11 February 2011** http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf
VIII.	**PAS 94:2013 Implementing privacy impact assessment (PIA) frameworks in radio frequency identification (RFID) application** . Guide – BSI and UK Department for Business Innovation & Skills – May 2013
IX.	**Fair Information Privacy Principles - PRIVACY POLICY GUIDANCE MEMORANDUM** December 29, 2008 - U.S. Homeland Security **http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf**

Appendix 1: BYOD in the cloud ï 2013 CSA Italy and CSA New Zealand Chapters Survey

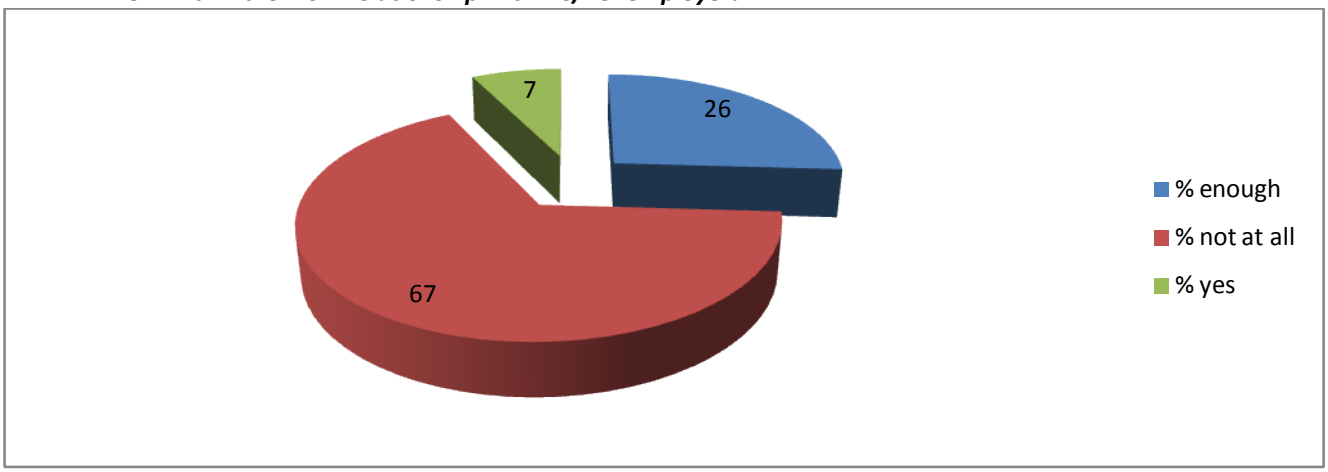
At the beginning of this study a specific survey has been prepared, run in May and June 2013 (in Italian and in English), with the aim to solicit attention from all interested parties within the groups of CSA Italy and CSA New Zealand fellows.

Here follows a summary of the responses obtained.

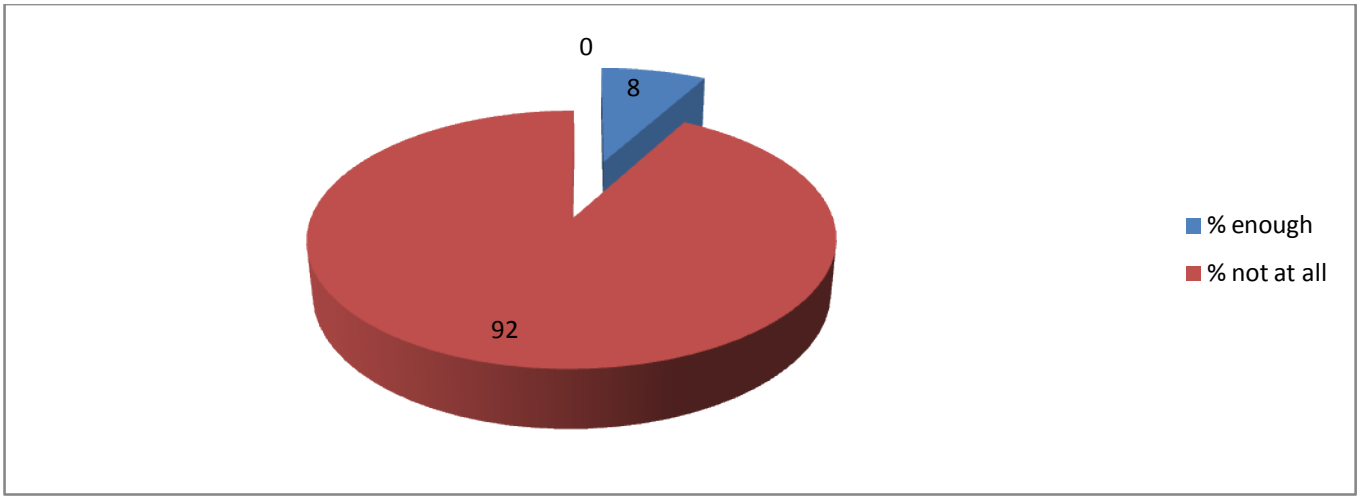
1. **Ritieni che le aziende siano consapevoli della necessità di applicare sul BYOD controlli di sicurezza in linea con la applicabile normativa in materia di privacy e protezione dei dati personali?/*Do you think the companies are aware of the need of applying BYOD security controls in-line with the applicable privacy and data protection legislation?***



2. **Ritieni che i lavoratori siano consapevoli dei rischi privacy derivanti dall'uso di BYOD nel rapporto di lavoro con la propria azienda?/*Do you think the employees are aware of the privacy risks in using BYOD within the work relationship with his/her employer?***



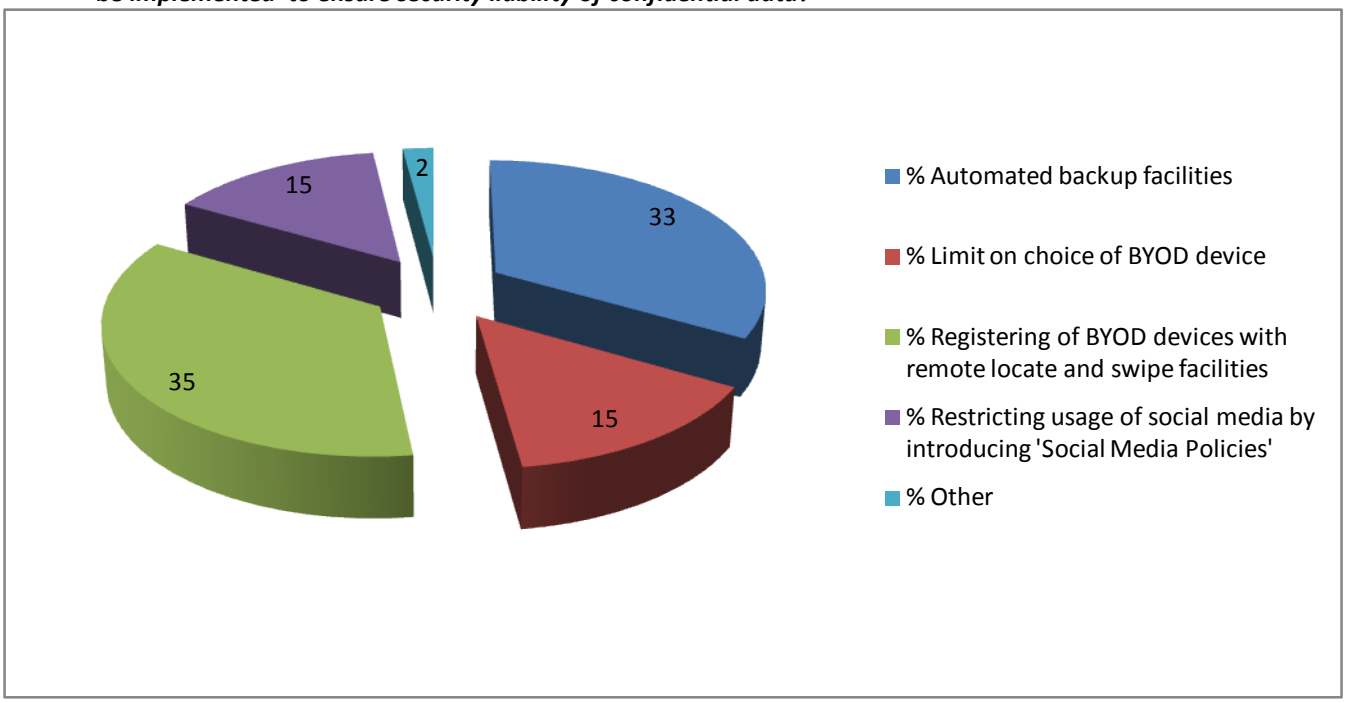
3. **Nel caso di violazione dei dati sul BYOD (esempio: BYOD rubato) ritieni che sia importante poter cancellare da remoto i dati in esso presenti?/*In case of BYOD security breach (example: stolen BYOD),do you think it is appropriate for an application to remotely wipe out the data?***



comments received:

- *Quale condizione necessaria, deve esserci una Policy aziendale che espliciti il wiping (insieme alle altre misure) e che tale Policy venga esplicitamente accettata dal Dipendente (o dalle rappresentanze sindacali)/ Necessary condition is the presence of a company policy expliciting the wiping (aligned with the other measures); that policy should be explicitly accepted by the employees (or by the Union representatives).*

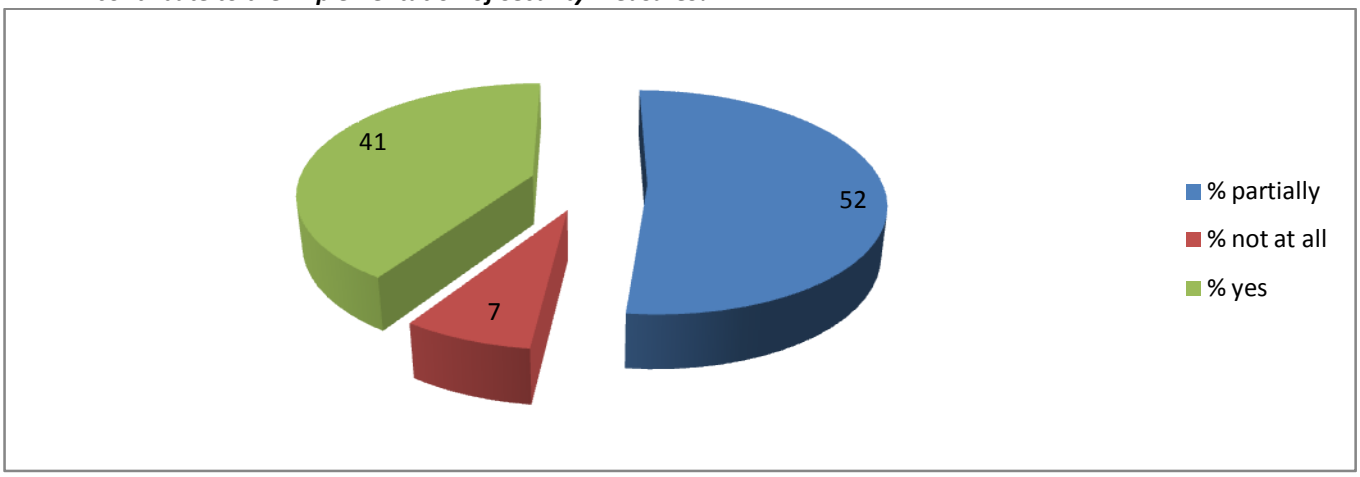
4. Quali delle seguenti misure BYOD pensi debbano essere applicate per implementare in concreto la responsabilità per la riservatezza dei dati?/*Which of the following BYOD measures do you think should be implemented to ensure security liability of confidential data?*



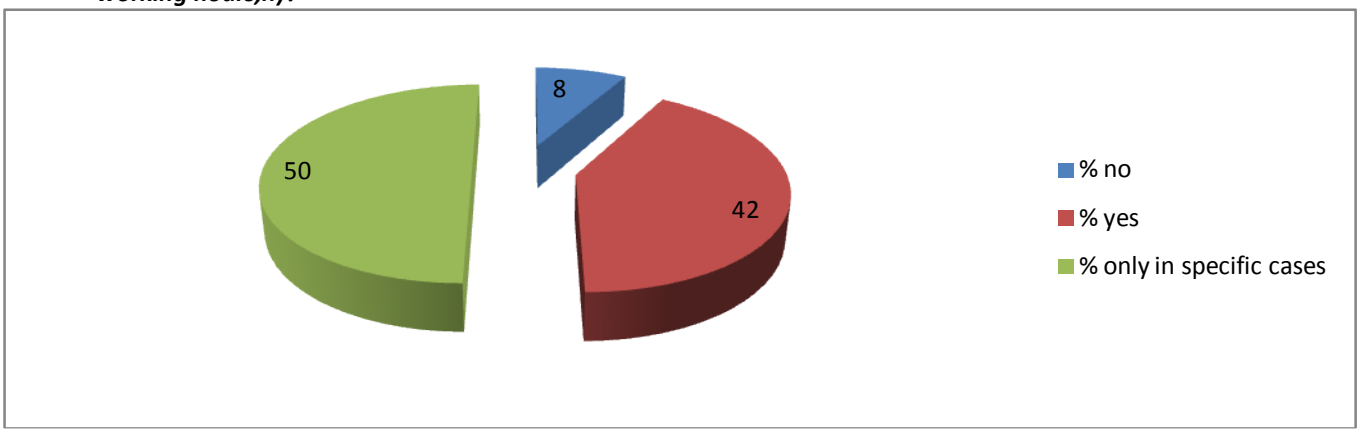
Other specification received:

1) Tecniche di partizione dei dati nel dispositivo applicando la modalità dual per distinguere i dati propri da quelli aziendali; 2) Lasciare la possibilità all'azienda di effettuare le patch necessarie; 3) Permettere all'azienda di far installare software aggiornati di antivirus, firewall, etc./ 1)Data partitioning techniques into the device, applying the dual modality in order to distinguish your own personal data from the company's ones; 2) Allow the company to insert patch as necessary into the device; 3) Allow the company to install up-to-date antivirus software, firewall, etc.

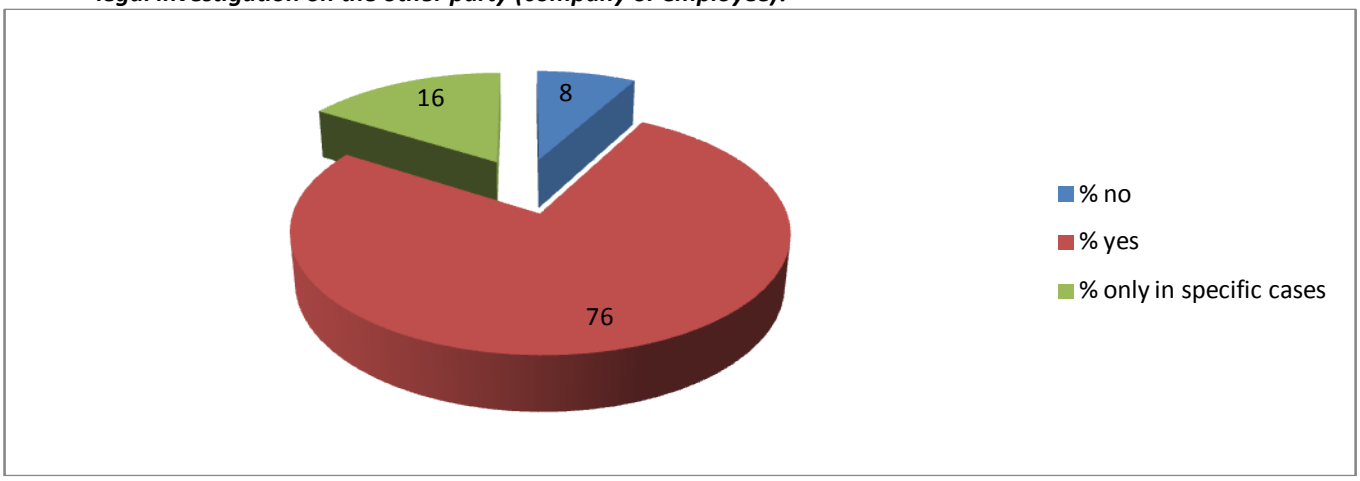
5. **Qualora al lavoratore sia consentito usare il BYOD anche per motivi personali: ritieni che egli debba in qualche modo contribuire alla implementazione delle misure di sicurezza?*Where the employee is allowed to use the BYOD also for personal reasons: do you think that he/she should in some way contribute to the implementation of security measures?***



6. **Considerando il caso in cui il BYOD sia assegnato dall'azienda al lavoratore, ritieni che le regole d'uso stabilite dall'azienda possano in qualche modo consentire il controllo sul lavoratore (es. sua geo-localizzazione, suo utilizzo di altre funzioni del BYOD durante l'orario di lavoro,..)?/*Considering the case where BYOD is assigned by the company to the employee, do you think that the company usage rules can somehow allow control over the worker (eg. geo-localization, use of other functions of BYOD during working hours,..)?***



7. **Ritieni che vi debbano essere specifiche prescrizioni di legge per tutelare i dati trattati da una parte (lavoratore oppure azienda) tramite un BYOD quando è in corso una investigazione legale sulla altra parte (azienda oppure lavoratore)?*Do you think that there should be specific legal requirements to protect the data processed by one party (the worker or company) via a BYOD when there is an ongoing legal investigation on the other party (company or employee)?***

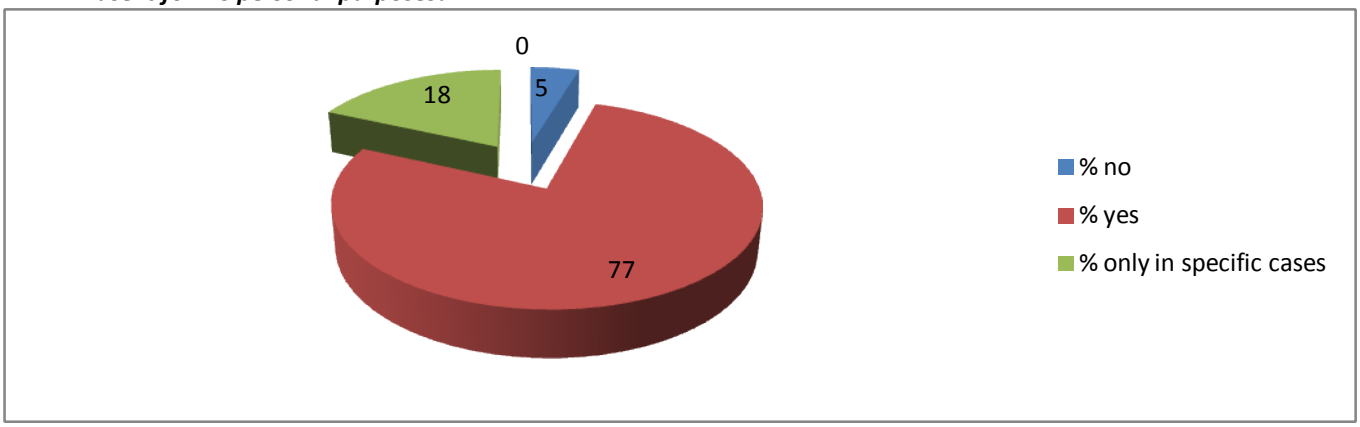


Comments received:

- *Il problema è serio: da una parte si dovrebbe investigare soltanto sui dati ed i profili utente relativi alla parte soggetta ad indagine, ma d'altra parte il problema legato al BYOD consiste proprio nel fatto che si viene a creare un bridge, volontario o involontario, tra il mondo personale e quello lavorativo. / The problem is serious: on one hand you should investigate just on data and user profiles regarding the part subject to investigation, on the other hand the matter connected to BYOD refers just to the bridge is going to create, voluntary or not, among the personal and the working worlds.*
- *Lato azienda è necessario stabilire un "Preservation Order"; Lato dipendente è utile stabilire formalmente la sua piena disponibilità dei dati contenuti nel dispositivo (anche qualora fossero dell'azienda) per finalità di difesa o similari. / From the company side it's necessary to establish a "Preservation Order"; from the employee side it is helpful formally establish his/her fully availability the device's data contents (even if those data are of the company) to defense purpose or similar.*
- *Esistono già delle leggi e sono commisurate all'effettivo proprio utilizzo degli apparati BYOD e NON. E' necessario invece inserire le responsabilità legislative in un framework BYOD, per esempio costituito da passi che concretamente verifichino l'utilizzo dei dati (rispetto all'Apparato: Dove è utilizzato, Chi lo utilizza, Con quale tecnologia - Wi-Fi, Mobile, Wired,… - in che Contesto - Company Policy, Public Body Regulation,... - e infine con quali dati - Social, Cloud/SaaS, DC/VDI,... Questo permette agli utenti di essere configurati, come status di utilizzo, all'interno di un ciclo di vita che potrebbe essere (è solo un'ipotesi, il ciclo di via può essere definito ad-hoc per l'azienda): Limited, Basic, Advanced, Full BYOD. / Laws already exist, which are commensurate to the effective utilization of BYOD, and other devices. Still it is necessary insert legislative responsibilities in a BYOD framework, for example made by steps verifying concretely the data utilization (in respect to the device: where it is used, who is going to use it, with which technology – Wi-Fi, Mobile, Wired,… - in which context – Company Policies, Public Body Regulations,… - and at last with what data – Social, Cloud/SaaS, DC/VDI,… That permits to*

users to be configured, as status of use, inside a life cycle which could be (it's just a theory, life cycle might be defined ad-hoc on a company-based way): Limited, Basic, Advanced, Full BYOD.

8. **Ritieni sia possibile che il lavoratore usi il BYOD fornito dalla societá per navigare sul web anche per motivi personali?/*Do you think is it possible for the employee to use BYOD issued by the company to use it for his personal purposes?***



Comments received:

- *In realtà qui ci troviamo di fronte ad un'antitesi: il termine BYOD significa 'Bring Your Own Device', ovverosia utilizza il tuo device personale anche per scopi aziendali. Ciò significa che l'utente può fare ciò che vuole del proprio dispositivo, ed in aggiunta può fare ciò che l'azienda autorizza. Volendo in ogni caso allargare il concetto anche al contesto opposto (ovverosia a quello in cui il dispositivo è aziendale e ne viene concesso l'utilizzo anche per scopi personali) si torna al caso ormai datato in cui l'azienda concede al collaboratore, come benefit, l'utilizzo del telefono aziendale anche per telefonate personali. / Actually here we have an antithesis: BYOD means "Bring Your Own Device", in other words, use your personal device also for business purposes. This means that the user can do whatever he/she wants with his/her device, and moreover he/she can do what the company approves. Broadening the horizons to the opposite context (this means when the device is owned by the company and the user can utilize it also for personal purposes) we go back to the dated example where the company grants to the employee, as a benefit, the use of a business mobile phone even for personal calls.*
- *Altrimenti non si ci sarebbe un gran problema e, quindi, non si parlerebbe tanto di BYOD. Ed è proprio questa "libertà" che fonda un po' tutta l'attenzione circa la sicurezza nel concetto del BYOD. / Otherwise there would not be a problem and then we could not talk about BYOD as much. And exactly this "freedom" is what attracts all this security attention around the BYOD concept.*
- *Ma in piena coscienza degli obblighi e delle responsabilità / With fully awareness about duties and responsibility.*

9. **Per quanto riguarda i dati, se il lavoratore esegue upload sul web o su sistemi cloud (normalmente utilizzati per il lavoro) anche suoi dati personali, quali pensi che possano essere le conseguenze di un tale errore?/** ***Concerning the data, if the employee uploads on web or cloud systems (normally used for work) also uploads personal data, what do you think is the consequence of such mistake?***

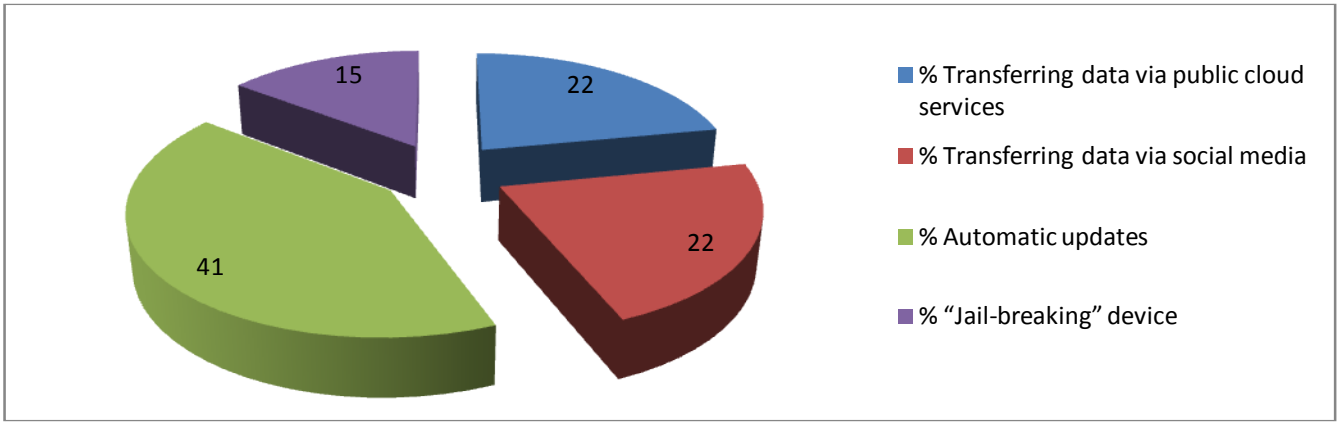
Comments received:

- *Accessi non autorizzati/controllati ai suoi dati personali / Not authorized/controlled access to his/her personal data*
- *Possibilità di caricare malware, aggiunta di contenuti non pertinenti / Possibility to load malware, inclusion of non-pertinent contents.*
- *violazione involontaria della privacy del lavoratore da parte dell'azienda e successiva cancellazione a cura del lavoratore; meglio sarebbe offrire uno spazio gratuito per i dati personali / Accidental violation of the employee privacy by the side of the company, and subsequent deletion by the employee; it should be better to offer a free space for personal data*
- *Possono essere più o meno gravi a seconda delle variabili del caso, ad ogni modo e facile che si verifichino se non altro degli equivoci / It could be more or less serious depending on the field variability, anyway it is easy to create at least some inappropriate misunderstadings*
- *Mettere a rischio sia i dati personali che quelli aziendali. / Put at risk personal data as well as business data*
- *La cosa và regolamentata: se la cosa è volontaria, di fatto ci si trova ad un utilizzo abusivo degli strumenti aziendali. In ogni caso, anche ipotizzando l'errore, l'utente rischia di perdere il controllo dei propri dati, che finirebbero archiviati, sottoposti a backup, indicizzati, etc. Inoltre i dati caricati dall'utente potrebbero costituire prova di reato a suo carico (ad esempio MP3, etc.). / The fact needs to be regulated: if it is a voluntary fact, then we have a misuse of business tools. In any case, even considering the error, the user could lose the control of his/her own personal data, which could be archived, backed-up, indexed, etc. Furthermore, the data uploaded by the user, could be a violation evidence against him/her (for example MP3, etc.).*
- *Security errors*
- *1) Sicuramente è una vulnerabilità che minaccia la sicurezza informatica aziendale (si possono introdurre virus, malware, etc.); / That surely is a vulnerability that threatens the company information security (a vehicle to introduce viruses, malware, etc.) 2) Si potrebbe concretizzare un accesso illegittimo o cmq non consentito per le finalità espresse; / There should be a concrete wrongful access or at least not-allowed access to the declared ends; 3) Si potrebbe configurare un utilizzo illegittimo di risorse aziendali; / There should be a potential wrongful use of company resources; 4) Si potranno configurare problemi legati alla disponibilità e/o legittimo utilizzo di tali dati, secondo le finalità espresse; / Potential issues about availiability and/or wrongful use of those data, based on the declared ends 5) Ci potrebbero essere ripercussioni anche dal punto di vista di altre leggi, es.: copyright; etc. / There should be impacts also regarding other laws, for ex.: copyright, etc.*
- *Non deve essere possibile predisponendo procedure e policy dedicate al backup su cloud (se pubblico o privato oppure entrambe i a discrezione dei diversi casi e controllori di BYOD / It*

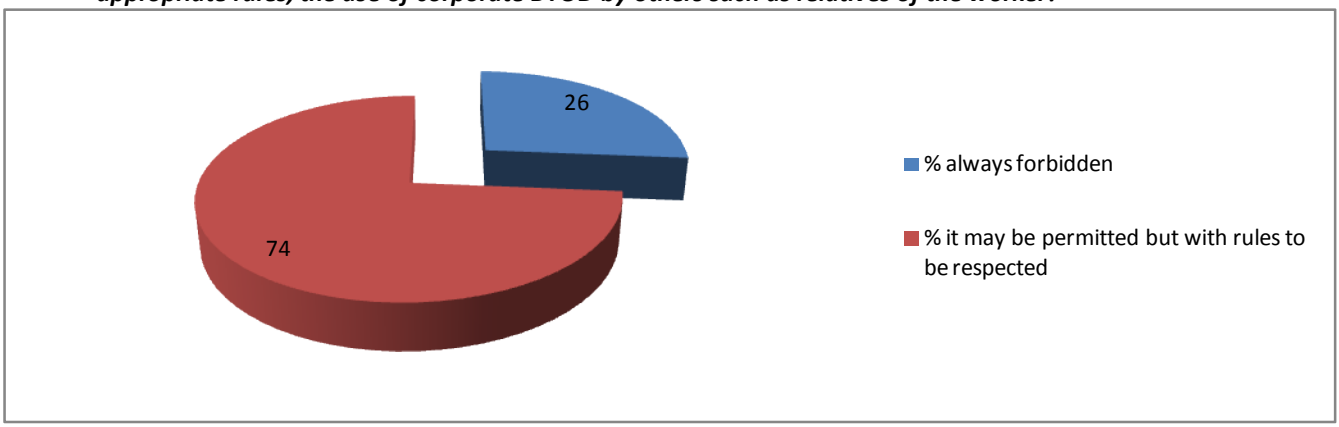
should not be possibile arranging policies and procedures specific to the backup on cloud (either public or private or both, at discretion of the different cases and BYOD controllers

- *Warning/alert*
- *Furto di identità /Identity theft*
- *ingerenza dell'azienda / intrusion by the company*
- *L'azienda deve porre in essere un quadro legale che le consente di evitare responsabiita' e agire direttamente per rimuovere i contenuti, senza rischi legali. / Companies should put in place a legal context that permits to prevent responsibilities and act directly to remove contents, without any legal risk.*
- *Conseguenze di violazione della privacy possibili se si fa upload di dati aziendali sensibili. Nessun "errore" se il lavoratore vuole fare upload di dati personali. / Potential privacy violation consequences in case of upload of confidential business data. No "errors" if the employee wants to upload personal data*
- *Se c'è questo tipo di errore vuole dire che non c'è conoscenza alla fonte. Il datore di lavoro deve essere certo che ogni lavoratore che entra nella sua azienda conosca le policy per l'utilizzo dei beni aziendali. / If there is this kind of error, that means that there is no knowledge at the source. The employer needs to be sure that each employee enters its company knows the personal data policies*
- *E' necessario che l'utente abbia la possibilità di optare per la configurazione di upload più congeniale e di poterla, all'occorrenza eliminare / It is essential that users have the possibility to choose the upload configuration the most suitable to him/her and to be able, if necessary, to delete it. - http://cloudbestpractices.net/profiles/blogs/maas-implements-small-data-and-enables-personal-clouds.*

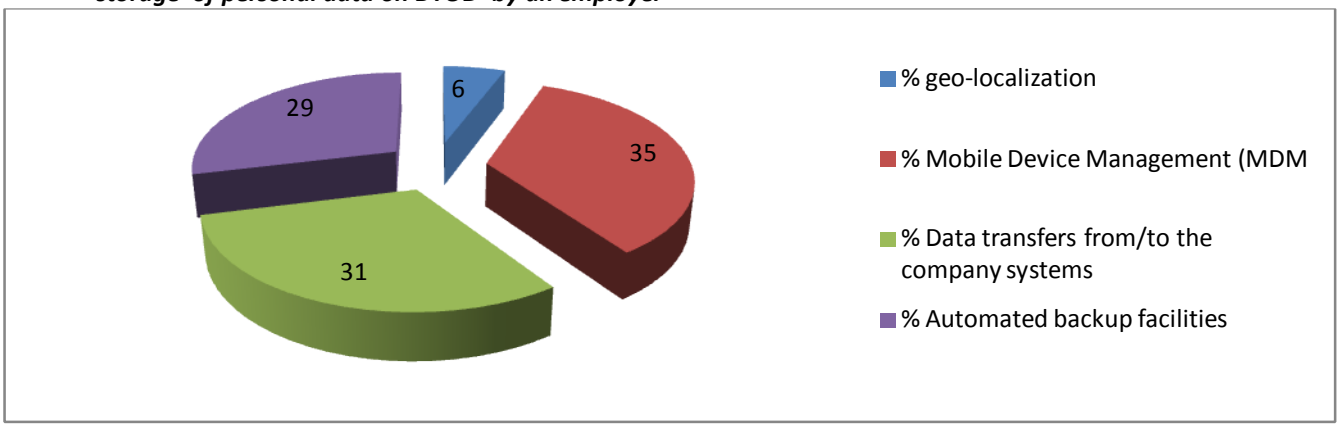
10. Quale fra i seguenti ritieni un utilizzo corretto di un dispositivo elettronico? / *What would you consider to be appropriate usage of your electronic device?*



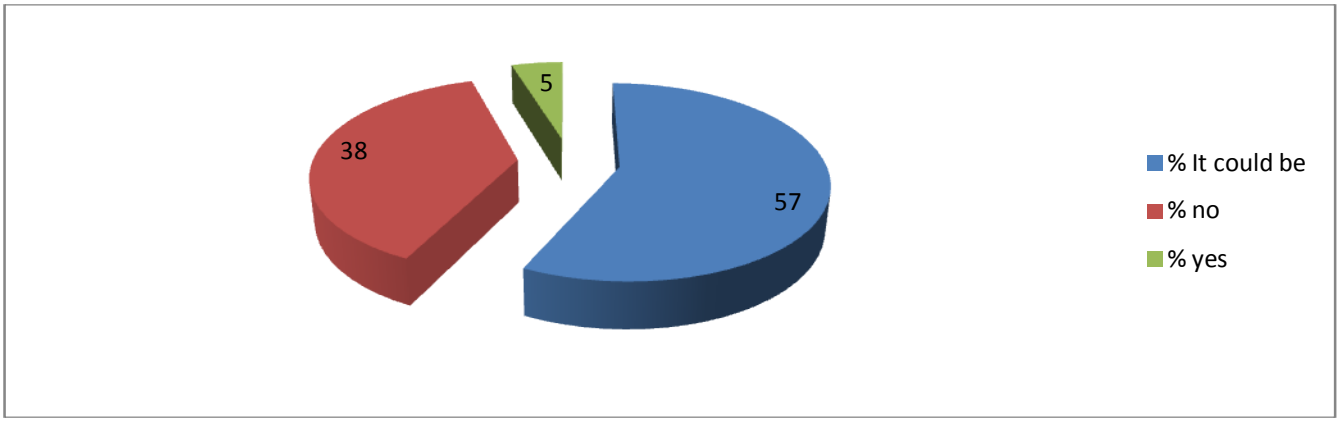
11. **Pensi che debba essere ammesso, anche se con apposite regole, l'uso del BYOD aziendale da parte di altri ad esempio I parenti del lavoratore? /*Do you think that it should be admitted, although with appropriate rules, the use of corporate BYOD by others such as relatives of the worker?***



12. **Quale ritieni che possa essere motivo giustificabile di "monitoraggio e conservazione" dati personali sul BYOD, effettuato dal datore di lavoro?/*Which would you consider to be 'justifiable monitoring and storage' of personal data on BYOD by an employer***



13. **Ritieni che l'utilizzo forzato di questi dispositivi possa portare ad una selezione impropria dei lavoratori?/ *Do you think that the mandatory use of BYOD may lead to an improper selection of workers?***



Appendix 2: BYOD LAWS CONCERNED ï EXECUTIVE SUMMARY

Here you can find the current release of the Catalog of law regarding BYOD under the perspective of data protection, privacy and worker monitoring (hereinafter the Catalog).

The Catalog intends to be a flexible and up to date information tool at international level: volunteers of CSA are encouraged to give their contribute for the law countries of their knowledge, the contact point for this initiative: **Team Leader of the Study**

Present Structure of the Catalog Content:

Sheet 1: Italy referenced laws

Sheet 2: UK referenced laws

Sheet 3: EU referenced laws (directives, regulations)

Sheet 4: Guides/ Opinions by relevant bodies

Sheet 1: Italy referenced laws

Number of the Law	196	58	300 (article 4)
Title of the Law	Codice in materia di protezione dei dati personali – Personal Data protection code	Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context - 1 March 2007	Workers' Statute
Type of law *(Decision, Regulation, Law, Legislative Decree, Order of Authority, ….)*	Legislative Decree	Italian Data Protection Authority measure	Law
Date of issue of the Law	30 June 2003	10/03/2007	20/05/1970
Hyperlink to official source where to find full text of the law *(no commercial website!)*	http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248	http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1408680	http://www.normativa.it/uri-res/N2Ls?urn:nir:stato:legge:1970-05-20;300
Sector of the Law (chose one of the following: **1) Work law** **2) Privacy law** **3) Other**	Privacy law	Privacy Law	Work law
Is it a national law transposed from an EU Law? *According to the case write: Y or N. In case Y please report the Number the Title the Type the Year of issue of the EU Law concerned*	Y: 95/46/EC - On the protection of individuals with regard to the processing of personal data and on the free movement of such data 2002/58/EC - Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)	N	N

Executive summary of the law requirement *Briefly describe what is the requirement*	Protections (informations, consensus to right exercise) to concerned people, security measures for data protections, limits to data transfer outside EC. In some cases, administrative obligations toward the Garante. Principal requirements: Data minimization, quality of data sections 3, 11; Information to concerned people, section 13; Rights exercise, section 7 and following; Concerned people consensus, sections 23, 24; Security measures, sections 31-35; Garante notify, sections 38 and following; Data transfer outside EC, 41 and following.	Below is a summary of the measure directly applicable: a. adopting and publicizing internal guidelines; b. adopting organisational measures, in particular to • carefully assess the impact on employees' rights; c. adopting technological measures, which include in particular, but are not limited to, the following: I. as for use of the Internet: • specifying which websites (by category) are considered to be related/unrelated to work performance; • configuring systems and/or using filters to prevent certain operations from being performed; • processing data in anonymous format and/or in such a manner as to prevent users from being immediately identified, by suitably aggregating the data in question; • retaining the data for no longer than is necessary to achieve organisational, production and/or security purposes; • providing for a layered approach to controls; II. as for email services: • making available email accounts to be shared by several employees, possibly along with individual accounts; • making available an ad-hoc account to be used by an employee for private purposes; • making available specific user-friendly functions to allow automatically sending out-of-office reply messages whenever it is known in advance that an employee will be absent from work, whereby such messages should provide details for contacting another employee and/or	For BYOD Purposes the relevant requirement: It prohibits the employer to use systems that allow remote control of work of employees

		department at the company/body in question; • where it is necessary to access the contents of email messages on account of pressing requirements related to work, and the relevant employee is absent from work unexpectedly and/or for a prolonged period, allowing the data subject (i.e. the employee in question) to entrust another employee (trusted party) with checking the contents of his/her email messages and forwarding such messages as are considered to be work-relevant to the employer (data controller). The data controller should keep specific records of these activities and the employee concerned should be informed thereof as soon as possible; • including a disclaimer in email messages to clarify, where appropriate, that they are not to be regarded as confidential and/or personal in nature, specifying whether the replies may be accessed by third parties in the sender's organisation; • providing for a layered approach to controls; 3. prohibits private and public employers from processing personal data by means of hardware and software systems with a view to the distance monitoring of employees, in particular by means of the following: a. the systematic scanning and recording of email messages and/or the respective external data apart from what is technically necessary to provide email services; b. the reproduction and systematic storage of the web pages visited by employees; c. keystroke pattern analysis and recording devices; d. hidden monitoring/analysis of laptops entrusted to individual employees; 4. pursuant to section 24(1), letter g. of the DP Code, sets out the cases in which personal, non-sensitive data may be processed in order to pursue the employer's legitimate interests also without the data subjects' consent – under the terms referred to in the premises	

BYOD impacts *Briefly describe why the requirement has impacts on BYOD*	Any BYOD deals with personal data so the employer will deal with requirements such as consensus and information.	- if detected a legitimate interest (Article 24 Paragraph 1 letter g) of the Code This provision prohibits employers to use systems to monitor the activities of their employees, except in cases provided for by the Data Protection Authority	it can't be used to control the worker
Does the requirement impose organizational/ procedural measures to the employer ? (example: provide information, prepare a company policy,…) *According to the case write: Y or N. In case Y briefly describe the required measure*	Y: Designation and instruction measures of responsibles, who have contact with personal data. In the context of home-based work and telework, employers will be required to ensure that the employees' personality and moral freedom are respected.	Y: see above executive summary of the provisions	Yes, an agreement whit the unions
Does the requirement impose to the employer communication /agreement with Unions and/or related Government Offices? *According to the case write: Y or N. In case Y briefly describe the required measure*	Y: Any control instrument of employees can be installed only after agreement with Unions. (Section 114, which recalls Section 4 300/1970 law)	Y: Since using BYOD there is the possibility of control by the workers, this measure raises the company from having to obtain the consent of the individual, as long as there has been an agreement with the unions	Yes, an agreement whit the unions and in caso of no agreement with unions, is the "Provincial Labour Inspectorate" to establish rules for the use of control equipment
Does the requirement impose to the employer communication /agreement with competent Authorities? (example: Data Protection Authority)	Y: In case of notification to the Garante or authorization from the Garante.	N	Y see above

According to the case write: Y or N. In case Y briefly describe the required measure			
Does the requirement impose technical measures? *According to the case write: Y or N. In case Y briefly describe the required measure*	Y: Autentication, Authorization, Encryption.		indirectly
Does the requirement impose behavioural measures to the employee? *According to the case write: Y or N. In case Y briefly describe the required measure*	N: There is no specific Section for the employee.	Y: fullfill the company policy in the use of email and internet and follow the security instructions	N
Sanctions *Please briefly describe, if any, the sanctions established by the Law (and refer the related Article)*	Administrative main sanctions: Providing No or Inadequate Information to Data Subjects - Up to 36.000 €; Submitting None or Incomplete Notification – Up to 120.000 €; Failure to provide Information or Produce Documents to the Garante – Up to 60.000 €. Main Criminal Offences: Unlawful Data Processing – Up to 3 years of imprisonment; Untrue Declarations and Notifications Submitted to the Garante – Up to 3 years of imprisonment; Unlawful Security Measures – Up to 2 years of imprisonment, up to 120.000 €; Failure to Comply with Provisions Issued by the Garante – Up to 2 years of imprisonment.	In the event of non-compliance of the provision is applied in the administrative sanction for payment of a sum from 30 000€ to 180 000€, However the minimun and maximum limits are to be applied in an amount equal to the two-fifths, if out any of the violations is of greater or lesser gravity	the worker can contact either the Labour Court that the magistrate, to request that the contractor is prevented by the use of these devices

Sheet 2: UK referenced laws

Nation of the Law *(if EU legislation write: EU)*	United Kingdom
Number of the Law	Chapter 36
Title of the Law	Freedom of Information Act
Type of law *(Decision, Regulation, Law, Legislative Decree, Order of Authority, ….)*	Act of Parliament
Date of issue of the Law	30th November, 2000
Hyperlink to official source where to find full text of the law *(no commercial website!)*	http://www.legislation.gov.uk/ukpga/2000/36/contents
Sector of the Law (chose one of the following: **1) Work law** **2) Privacy law** **3) Other**	Privacy Law Human Rights Law
Is it a national law transposed from an EU Law? *According to the case write: Y or N. In case Y please report the Number the Title the Type the Year of issue of the EU Law concerned*	N
Executive summary of the law requirement *Briefly describe what is the requirement*	Principal requirements: The Freedom of Information Act 2000 created a public "right of access" to information held by public authorities. It is the implementation of freedom of information legislation in the United Kingdom on a national level. S6 of the Freedom of Information Act 2000 provides that a company is publicly owned if: (a) it is wholly owned by the Crown, or (b) it is wholly owned by any public authority listed in Schedule 1 other than (i) a government department, or (ii) any authority which is listed only in relation to particular information. Public authorities have two main responsibilities under the Act: 1) They must produce a 'publication scheme', which is, in essence, a guide to the information they hold that is routinely made available to the public, such as prospectuses, almanacs and websites. Under the Freedom of Information Act 2000, 'information' includes all information held anywhere within an institution and does not have to be in the form of a specific document or structure, e.g. a database. The Information Commissioner must approve each authority's publication scheme. 2) They must deal with individual requests for information. Individuals already have the right to access their personal data, held on computer and in some paper files, under the Data Protection Act 1998. This is known as the 'subject access right'. The Freedom of Information Act permits individuals to access all other types of non-personal information that public authorities hold, subject to specific exemptions in the Act

BYOD impacts *Briefly describe why the requirement has impacts on BYOD*	
Does the requirement impose organizational/procedural measures to the employer ? **(example: provide information, prepare a company policy,…)** *According to the case write: Y or N. In case Y briefly describe the required measure*	Y: As well as the "general right of access", the Act places a duty on public authorities to adopt and maintain pro-active "publication schemes" for the routine release of important information (such as annual reports and accounts). The Information Commissioner must approve these publication schemes.
Does the requirement impose to the employer communication/agreement with Unions and/or related Government Offices? *According to the case write: Y or N. In case Y briefly describe the required measure*	Y: In relations to the European Union and the Human Rights Act 1998 regarding Article 10 on the right of freedom of expression.
Does the requirement impose to the employer communication/agreement with competent Authorities? (example: Data Protection Authority) *According to the case write: Y or N. In case Y briefly describe the required measure*	Y: To the **Information Commissioner's Office** (ICO; stylized as ico.). ICO is an independent regulatory office dealing with the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 across the UK; and the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 in England, Wales and Northern Ireland and, to a limited extent, in Scotland.
Does the requirement impose technical measures? *According to the case write: Y or N. In case Y briefly describe the required measure*	
Does the requirement impose behavioral measures to the employee? *According to the case write: Y or N. In case Y briefly describe the required measure*	Y: Via the publication schemes imposed and approved by the Information Commissioner.
Sanctions *Please briefly describe, if any, the sanctions established by the Law (and refer the related Article)*	

Sheet 3: EU referenced laws (directives, regulations)

Nation of the Law *(if EU legislation write: EU)*	EU	EU	EU
Number of the Law	46	58	611
Title of the Law	Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: **Data Protection Directive**	Directive 2002/58 on Privacy and Electronic Communications, otherwise known as **E-Privacy Directive** (amended by Directive 2009/136/EC)	COMMISSION REGULATION (EU) No 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications
Type of law *(Decision, Regulation, Law, Legislative Decree, Order of Authority, ….)*	Directive	Directive	Regulation
Date of issue of the Law	24 October 1995	12 July 2002	of 24 June 2013
Hyperlink to official source where to find full text of the law *(no commercial website!)*	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF
Sector of the Law (chose one of the following: 1) Work law 2) Privacy law 3) Other	Privacy law	Privacy law	Privacy law
Is it a national law transposed from an EU Law?	N	N	N

According to the case write: Y or N. In case Y please report the Number the Title the Type the Year of issue of the EU Law concerned			
Executive summary of the law requirement *Briefly describe what is the requirement*	The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union directive which regulates the processing of personal data within the European Union. It is an important component of EU privacy and human rights law	The Electronic Privacy Directive has been drafted specifically to address the requirements of new digital technologies and ease the advance of electronic communications services. The Directive complements the Data Protection Directive and applies to all matters which are not specifically covered by that Directive. In particular, the subject of the Directive is the "right to privacy in the electronic communication sector" and free movement of data, communication equipment and services. The Directive does not apply to Titles V and VI (Second and Third Pillars constituting the European Union). Likewise, it does not apply to issues concerning public security and defense, state security and criminal law. At present, the interception of data is covered by the new EU Data Retention Directive the purpose of which is to amend E-Privacy Directive.	This regulation sets common rules for telecoms operators and Internet services providers (Providers) for the notifications of personal data breach to the competent national authorities as well as to the subscribers and individuals.
BYOD impacts *Briefly describe why the requirement has impacts on BYOD*		Data breach with reference to the use of BYOD , see also EU Regulation 611 2013	Data breach in relation with the use of BYOD (publicly accessible electronic communications services)
Does the requirement impose organizational/procedural measures to the employer ?	N	N	N

(example: provide information, prepare a company policy,…) *According to the case write: Y or N. In case Y briefly describe the required measure*			
Does the requirement impose to the employer communication/agreement with Unions and/or related Government Offices? *According to the case write: Y or N. In case Y briefly describe the required measure*	N	N	N
Does the requirement impose to the employer communication/agreement with competent Authorities? (example: Data Protection Authority)	N	N	Y, data breach notification to the competent national authority and also to subscribers/indviduals when it is likely to adversely affect the personal data or privacy of a subscriber or individual

According to the case write: Y or N. In case Y briefly describe the required measure			
Does the requirement impose technical measures? *According to the case write: Y or N. In case Y briefly describe the required measure*	N	N	Y, data encryption or hashing as a mean for derogation regarding the data breach notification to subscriber/individual
Does the requirement impose behavioural measures to the employee? *According to the case write: Y or N. In case Y briefly describe the required measure*	N	N	N
Sanctions *Please briefly describe, if any, the sanctions established by the Law (and refer the related Article)*	Sanctions are disciplined in chapter III Article 24: the member states have to adopt suitable measures to ensure the full implementation of the provisions of the Directive and shall lay down the sanctions to be impose in case of infringement of the provisions adopted pursuant to the Directive.	The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.	No further sanctions other than what specifically defined in Directive 2002/58/EC

Sheet 4: Guides/ Opinions by relevant bodies

Country	Type	Organization	Title	Hyperlink
UK	Guideline	ICO (UK Data Protection Authority)	Bring your own device (BYOD)	http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod
UK	Guideline	ICO (UK Data Protection Authority)	Cloud computing guidance	http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing
EU	Opinion	WP 29	Opinion 02/2013 on apps on smart devices	http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
EU	Opinion	WP 29	Opinion 03/2013 on purpose limitation	http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
EU	Opinion	WP 29	Opinion 05/2012 on Cloud Computing	http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
EU	Opinion	WP 29	Opinion 15/2011 on the definition of consent	http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf
Italy	Guideline	Italian Data Protection Authority	Fatti smart! Le indicazioni del Garante per tutelare la tua privacy quando usi smartphone e tablet (Be smart! The indications of the Italian DPA for the protection of your privacy when using smartphones and tablets)	http://www.garanteprivacy.it/fattismart
Italy	Guideline	Italian Data Protection Authority	CLOUD COMPUTING – PROTECT YOUR DATA WITHOUT FALLING FROM A CLOUD Guidance from the	http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906181

			Italian DPA to businesses and public bodies	
Italy	Guideline	Italian Data Protection Authority	La privacy dalla parte della impresa (Privacy from the side of the enterprise)	http://www.garanteprivacy.it/documents/10160/2416443/Vademecum-privacy-e-imprese.pdf
New Zealand	Code of practice	New Zealand Privact Commissioner	CLOUDCODE NEW ZEALAND CLOUD COMPUTING CODE OF PRACTICE	df

