JBN Seminar
Risk Assurance Services
Ethics and Compliance in Italy: trends and update 2019
13 March 2019
Introduction

➢ The modern global enterprises have an **increasing number of relationships and interdependence and create a complex and symbiotic network** of third parties, customers, employees, etc.

➢ In this context the **stakeholders** expect compliance and ethics function to protect the organizations. It is undeniable that the **importance of effective compliance has never been grater**: compliance failures can cause organizations to suffer huge reputational damage, high customer churn, and massive fine.

➢ **For these reasons an increase on regulatory compliance pressure** regarding third parties relationships, data protection matters, Health and Safety measures to be implemented by organizations, etc. is in place.

➢ To **protect against risks**, companies must identify their compliance needs, prioritize them according to risk based approach and define effective ad customize solution according to international/well recognized frameworks and models.

**Organizations with effective compliance programs are innovative, optimistic, and building a risk culture**
Ethics & Compliance matters checklist 2019 – General considerations

Five tough questions to ask about your organization’s state of compliance:

1. Does your organization’s senior leadership make to delivery of compliance and ethics a priority?

2. Is your organization’s senior leadership measured in any way on its commitment to compliance and ethics?

3. Does your organization’s existing risk assessment process capture the current state of compliance and ethics risk management with sufficient detail so as to power your planning and execution of necessary mitigation activities?

4. Does the structure of your organization’s compliance and ethics function truly enable and support key activities to address prioritized risk areas?

5. Does your organization’s Board and senior leadership provide meaningful oversight and support of the compliance and ethics function?

*PwC State of compliance Study
Section 1
Compliance with Italian rules: focus on the importance of third parties relationships
**Trends and main issues**

- **Increasing regulatory compliance pressure regarding third parties relationships.** Regulators around the world, for instance in the financial services domain, are significantly increasing their attention on the third party risks faced by their regulated entities.

- It is interesting to note the **increasing** Regulators **attention on** the subcontractors supporting the third party business ("fourth parties").

- Relationship with **third parties brings risks** such as bribery and corruption, disruption to continuity of operations, environmental or labor concerns and legal or reputational damage.

- To **protect against risks**, companies must choose their third parties with care, ensure they operate to required standards and monitor their performance (**third parties risk management**).
**Relevant Italian Laws**

Third parties relationships are relevant for a number of Italian laws; hereafter are summarized some examples of relevant laws that entails the implementation of adequate controls and monitoring activity over third parties.

**Italian Legislative Decree n. 231/2001**

Legislative Decree No. 231 dated 8 June 2001 (DLgs 231/01) establishes a direct responsibility of entities - substantially equivalent to criminal liability - for certain offences committed in the interest or to the advantage of the entity by physical persons holding senior executive or subordinate positions, but also by external parties like consultants, suppliers, partners, the sales network, and all those that – although external to the organization – operate directly or indirectly for the company. It also sets out fines and other measures - debarment sanctions, confiscation of the profit from the offence, publication of the sentence - that can be imposed on the entity.

The entity is not liable if it can prove that:
- the management adopted and effectively implemented an organizational, management and control model, prior to the offence, able to prevent those types of crimes from being committed (“Model 231”);
- the task of overseeing the functioning of and compliance with the Model has been assigned to a body of the entity (“Organismo di Vigilanza”);
- the perpetrator committed the offence by not complying with the Model;
- the “Organismo di Vigilanza” did not perform or performed insufficient oversight.

The catalogue of crimes relevant for the DLgs 231/2001, is wide and heterogeneous and the most of entity’s processes and activities are exposed to crimes commission risk.

Since third parties operate within sensitive activity areas on behalf of or in the interest of the organization, they are addressee of the Model that engage them to act in fair and transparent behaviors when performing their activities, in line with the ethical and social values that inspire the Company in pursuing its corporate purposes, and to prevent the risk of commission of the crimes set out in the Law.

In addition, most of the offences relevant for the DLgs 231/01, presuppose a relationship with a third part, for example
- Organized crimes;
- Crimes connected to terrorism or subversion of democracy;
- Offences involving relationships with Public Administrators/Government;
- Bribery among private individuals.
**Relevant Italian Laws**

**Anti bribery regulation**

Italian Law governs the **private-to-public bribery offenses**, the **private bribery** and **incitement to private bribery**.

In addition Article 25 of Legislative Decree 231/2001 envisages the company’s administrative liability in case of corruption and bribery committed in the interest or to the advantage of the company by directors, executives and their subordinates, agents and other individuals acting on behalf of the legal entity.

Italy has also implemented its commitments to the Criminal Law Convention on Corruption (1999) and to the UN Convention against Corruption (2003) by Law 190/2012, by which a few provisions of the Italian Criminal Code concerning corruption were amended and other new provisions were introduced (eg the undue induction to give or promise a benefit by public officials).

Is easily understandable that the **third parties relationships are critical for bribery and corruption risks**; is embedded in the regulation that to protect against bribery and corruption risks, companies must choose their third parties with care, ensure they operate to required standards and monitor their performance.

**Antimafia law**

Legislative Decree no. 159/2011 introduced the ‘**Code of antimafia law**, that contains relevant preventive antimafia measures meant to combat the mafia.

Among the **asset protection measures**, there are those introduced **in case** of suspected of **Mafia infiltration**, it means that situation where sufficient indications exist to believe that the free exercise of a determined economic activity is directly or indirectly subject to criminal intimidation or conditions of subjection.

In these situations, the court may order the **judicial control** of the economic activities by judicial administrators, appointed for a period.

**To avoid situation on Mafia infiltration**, is essential that organizations **implement effective controls to manage the risks to deal with counterparties belonging to criminal organizations.**
### Anti money laundering

The **anti-money laundering legislation in Italy** is contained in **Legislative Decree no. 231/2007**.

Legislative Decree No. 90 of 25 May 2017, has implemented in Italy the **Fourth European Money Laundering Directive** (Directive 2015/849/EU on the prevention of the use of the financial system for the purpose of money laundering or terrorism financing (the Fourth EU Directive)). One the most **important news introduced** by Legislative Decree no. 90/2017, **concerns** the **Customer due diligence requirements** that consists of the following activities:

- ✓ identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from a reliable and independent source;
- ✓ identifying the beneficial owner and verifying his or her identity;
- ✓ obtaining information on the purpose and the intended nature of the business relationship or professional service;
- ✓ conducting of ongoing monitoring in the course of the business relationship or professional service.

The “**categories of obliged subjects**” identified by the Decree, as:
- banking and financial intermediaries and other financial operators, including the Italian branches having their registered office in a foreign country;
- professionals such as accountants, auditors and, under certain conditions, notaries public and lawyers;
- “other non-financial operators” i.e. antique dealers, art dealers, collection agencies, etc.; and - gaming service providers.

Therefore, the **obliged subject are requested to comply with AML law, to identify the relevant third parties and assess the related relevant risks**.

Please note that **money laundering crime is relevant also company’s administrative liability** (ex Legislative Decree 231/2001) and then **relevant for any organization and business**.
Main area / processes at risk

The most of Company areas and processes are exposed to risks connected to third parties relationships.

Depending on the Business Industry, some areas could be considered more risky than others.

Following are indicated some examples of “sensitive areas”:

- **Procurement** (including relation with subcontractors)
- **Logistic**
- **Human resources**
- **Sales** (including relations with sales agents, intermediaries, etc.)
- **HSE**
- **Joint Ventures and Partnerships**
- **Sourcing**
- **Administration and Finance**
How to manage Third Parties Risks?

The most common best practices and methodological frameworks, recognize the importance of implementing an effective third parties management process, for identifying, engaging and managing third parties. The main components that form the core of good practice in third party management include:

**Identification of third parties**

Identify and register all third parties and collect, analyze and store relevant information about them.

The company’s third party population can include:

- Vendors/suppliers
- Distributors/resellers
- Joint venture partners/consortium partners
- Advisors and consultants (tax, legal, financial, business)
- Service providers
- Contractors/subcontractors
- Lobbyists
- Marketing and sales agents
- Customs or visa agents
- Other Intermediaries

**Risk assessment**

Identify, mitigate and monitor the risks and risk factors attached to different types of third parties and use this information to design the criteria used in due diligence. A “one-size-fits-all” approach to third party management diverts focus from the highest risk third parties and may result in inadequate supervision or unethical behavior that damages the company.

**Pre-qualification**

Adopt a comprehensive and consistent approach to engaging third parties to ensure that engagements are made to desired standards and that procedures are tailored to the different types of identified risks.

**Contract**

The contract with the third party communicates explicitly the company’s expectations regarding ethical behavior, establishes rights, specifies requirements and processes for monitoring, remediation, termination and exit.

**Monitoring**

Perform periodical Due Diligence review. Carry out periodical audits on all high risk third parties (Audit rights are a standard part of agreements with all third parties)

**Communication and training**

Provide communications and training to internal and external resources.

---

* Due diligence is a term used to describe background investigation conducted on a third party which a company is considering contracting with.

---

*PwC*
How PwC RAS can help you

In response of the above mentioned Compliance needs, PwC can support you about the following matters that could be relevant for Organizations.

PwC RAS can provide methodological and operative support, in designing a third party governance & risk management model and in performing the related activities (analysis, reporting, monitoring, etc.)

PwC RAS can provide support in implementing an Antibribery management system, according to the requirements set by the standard ISO 37001: 2016. Such standard specifies a series of measures to help organizations prevent, detect and address bribery.

PwC RAS can provide support in:
- Set up Internal Audit function
- Full Internal Audit outsourcing
- Internal Audit Co-sourcing
- Quality Assurance Review of Internal Audit Function

PwC RAS can provide support in:
- Set up Internal Audit function
- Full Internal Audit outsourcing
- Internal Audit Co-sourcing
- Quality Assurance Review of Internal Audit Function

PwC RAS can provide support in designing and implementing an effective Organizational, Management and Control Model according to the Italian Legislative Decree no. 231/2001 (including Code of Ethics).

PwC RAS can provide support in design, implementing and managing an effective Whistleblowing Process, in compliance with the law and the relevant compliance programme implemented (i.e Antibribery management system, Organizational, Management and Control Model 231/2001, etc.)
Section 2

How to effectively manage issues related to Health and Safety at work
Health and Safety at work
Some figures regarding Italian environment

Some figures
In Italy, every year, there are over 590,000 complaints related to injury at work, many of which have death consequences for workers.

A growing number of Entities are adopting a Health and Safety Management system (HSMS) to reduce risks and incidents and to strengthen the compliance with applicable regulations on health and safety, which in Italy is the Legislative Decree 81/08.

In March 2018, the new ISO 45001:2018 Standard was released, which is the first certifiable ISO Standard for HSMS.

The new Standard will replace the British Standard OHSAS 18001:2007 and contains the internationally established criteria by ISO, similar to other international standards such as ISO 9001:2015 (quality) and ISO 14001:2015 (environment).

~ 590000 injuries
Injury complaints, 78% of which come from the industrial sector (year 2017)

~ 950 deaths
Fatal injury complaints, 83% of which come from the industrial sector (year 2017)
Health and Safety at work
Some figures regarding Italian environment

The new ISO 45001 Standard aims to help organizations prevent injuries at work, whose occurrence expose them to significant risks, including:

- **application of penal sanctions** towards Employers, Safety Delegates, and HS Managers (Prevention and Protection Service);
- **corporate liability** of Entities in accordance with Legislative Decree 231/2001;
- **reputational damage** and difficulties in managing contractual relations with suppliers and customers.
Health and Safety at work
The key components for HSMS based on ISO standards

The ISO 45001:2018 Standard has the same key components as all other ISO Standards, which significantly facilitates the process of their integration, especially for the prevention of related issues (e.g. worker safety and environmental protection).

Leadership
- Leadership and commitment
- Policy on health and safety at work
- Organization of roles, responsibilities and authority
- Involvement of workers

Organizational context
- Knowledge of the organization and its context
- Knowledge of workers’ and other stakeholders’ needs and expectations
- Setting of objectives of the management system, related to health and safety at work

Operating activities
- Operational planning and control (threats elimination and risk reduction in terms of safety at work)
- Change management
- Procurement
Health and Safety at work
The key components for HSMS based on ISO standards

Planning
- Identification of actions for the management of risks and opportunities
- Identification of objectives and planning of activities for their achievement

Monitoring and measurement
- Monitoring, measuring, analyzing and evaluating performance
- Internal audits
- Management review

Support
- Resources identification
- Competences definition
- Responsibility definition
- Communication channels

Progress
- Injuries, non-conformities and management of corrective actions
- Continuous improvement
Health and Safety at work

Benefits

*Economic benefits:*

The correct prevention and management of issues related to health and safety at work lead to a reduction in costs related to the decrease of accidents, injuries, interruption of production processes, as well as possible advantages in the tendering process.

*Funding access:*

Entities investing in prevention of health and safety issues may have access to funds made available by Governmental institutions (i.e. INAIL) through calls for proposals.

*Insurance benefits:*

The correct functioning of the HSMS represents an incentive that can be used by insurance companies to obtain lower premiums.

*Compliance:*

The adoption of a 231 Management and Control Model based on tools and controls, such as those provided by the ISO 45001 Standard, can reduce or exempt the corporate liability of the Entity according to Law Decree 231/01.
Health and Safety at work
ISO 45001: main news

Following the publication of the ISO 45001 Standard, those who:

1. are already equipped with an HSMS according to the OHSAS 18001 Standard
   - Will have to **adapt their HSMS** within 3 years of its publication. Otherwise, they will lose their certification and will have to reperform the whole process.

2. want to implement an HSMS
   - Will necessarily have to **adopt the new ISO 45001** after the transition period.

**Context analysis**

The new ISO 45001 requires:

- the identification of possible **external problems**
- the detection of **needs and expectations of third parties** such as authorities, trade unions, holding companies, suppliers, customers, etc.

**Leadership and commitment**

The commitment of top management is no longer limited to the definition of a Policy but requires **greater involvement** in the following activities:

- alignment and compatibility between the strategic objectives and the objectives of the HSMS
- **Integration of HSMS requirements and objectives** into business processes

**Contractors and outsourcing**

The new ISO 45001 requires greater attention in the **management of relations with suppliers** and outsourced processes.

**Integration with processes**

The new ISO 45001 requires a strong integration between the requirements of the standard and the business processes including:

- **the use of procedures**
- **the appropriate assessment of skills**
- **the definition of specific requirements related to procurement**
- **the provision of engineering controls**
Health and Safety at work

How can we assist you?

Thanks to our resources, qualified and specialized in the safety at work matters, as well as our consolidated and diversified experience, we are able to assist organizations in all the steps required, from the design of the HSMS to the certification by a 3rd party.
Health and Safety at work
Our methodological approach

Does the organization already have an HSMS?

Yes

Gap Analysis
Identify misalignments to the new ISO 45001 standard

Implementation
Identify corrective actions for compliance with the requirements of the new ISO standard

Execution
Implement all mechanisms to ensure the proper functioning of the HSMS

No

Identify stakeholders
Define the HSMS policy
Identify the applicable standards
Define the Audit Plan

Identify and analyze the context
Identify risks and opportunities
Define the HSMS objectives
Perform audits and reviews
Health and Safety at work
Our Transition to ISO 45001 – Case History

- **Sector:** Renewable energy
- **Project objectives:** transition to HSMS based on ISO 45001 from BS OHSAS 18001.
- **Activities performed:**
  - Gap Analysis
  - Assistance in the implementation of gaps identified
  - Integration of HSMS in Company’s Integrated Management Systems (ISO 14001/ISO 9001, etc.)
- **Goal achieved:**
  - Unique Management System integrated with all ISO Standards implemented by the Company
  - Reduction and simplification of documentation
  - Stronger compliance with HS regulation
Section 3

GDPR and Cybersecurity update
Data protection – Italy update

The entering into force of the Italian Legislative decree no. 101/18.

Finally on September 19th, 2018 the Italian Legislator approved the Legislative decree no. 101/18 which is aimed at adapting the ancient Italian “Privacy Code” (the Legislative decree no. 196/03) to the new provisions concerning the processing and management of personal data set forth by the New European Regulation 2016/679 (the GDPR).

Provided that the EU Regulation contains rules and provisions applicable all over the Europe, each Member State shall, in compliance with this latter, adopt national Law in order to coordinate ancient provisions with the new ones.

Some of the main interventions has been already touched but, in addition to those, the Italian Legislative decree of September 2018 introduces some key items.
Data protection – Italy update

D.lgs. 101/2018 (“Decreto di armonizzazione”)

Through the Gazzetta Ufficiale n. 205 of 4th September 2018, the Legislative Decree no. 196/2003 (Italian personal data protection Code) has been repealed and it has been published the D.lgs. 101/2018 (“Decreto di armonizzazione”).

The regulatory update was mainly focused on the modification, also with due formalities, of several articles of the Code in order to incorporate and align the Legislative Decree 196/2003 to the GDPR.

The minor who has completed the fourteen years can express consent to the processing of their personal data in relation to the direct offer of services of the information society, otherwise the consent of the person exercising parental authority.

Such data can be processed only if authorized by a law or regulation, which provide appropriate guarantees for the rights and freedoms of the interested parties.

The legislator has delegated the Guarantor to prepare ethical standards in the context of work relations (and not only).

Data processed (and therefore also collected) in violation of the privacy regulations (national and European) can not be used (processed) in any way except by the same Guarantor for the purpose of investigations into an infringement.
The first few months of application of GDPR

Assessment on GDPR after 1 year (1/2)

On January 30, 2019, the Italian Data Protection Authority (the “DPA”) published on its official website a report of the results registered in the first 8 months of application of the GDPR, highlighting, in particular, the following information:

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications of the contact information regarding DPO</td>
<td>43,269</td>
</tr>
<tr>
<td>Complaints and notifications</td>
<td>4,704</td>
</tr>
<tr>
<td>Data breach notifications</td>
<td>630</td>
</tr>
<tr>
<td>Contacts with the Public Relations Office</td>
<td>13,835</td>
</tr>
</tbody>
</table>
**Data protection**

**Some of the key items**

**BASE FOR THE PROCESSING**

The Decree clarifies that, with regard to processing activities carried out in the exercise of public interest or connected with the exercise of official public authority, the legal basis may be constituted exclusively by a rule of law or regulation.

**DESIGNATED SUBJECTS**

The Controller and the Processor shall delegate certain tasks and functions to which they are subject to intermediate persons who always will act under their authority. *(Please refers to next slides.)*

**CURRICULA**

The information and consent to the treatment are not due in case the interested parties spontaneously transmit their curricula for the purpose of any establishment of an employment relationship. The due information shall be provided to the data subject at the time of the first contact after sending the curriculum.
Data protection

Some of the key items

The Decree, in modifying the Italian Privacy Code, coordinates with the system of administrative sanctions provided for in the Regulation.

The Italian Guarantor is responsible for the definition and adoption of the sanctions. Within 30 days (60 if the offender resides abroad), the offender and the jointly and severally debtors may settle the dispute in accordance with the provisions of the Guarantor (if any) and through the payment of an amount equal to half of the imposed sanction.

The Legislative decree also inserts some additional criminal offences for the most serious violations as well as two additional articles (i.e. article no. 167bis and 167ter) due to the growing of cyber attacks on structures that process large amounts of personal data.

The Legislative decree provided for a transitional period of 8 months starting from its entering into force (i.e. form September 2018 to May 2019) in which the Italian Guarantor in applying the administrative sanctions established by the Regulations, will take into consideration the fact that the new provisions are newly introduced.
Data protection

“Data Breaches”

What is meant by “Data Breach?”

This term refers to a breach of security that leads accidentally or unlawfully to the destruction, loss, modification, unauthorized disclosure of or access to personal data transmitted, collected or otherwise processed.

Principal examples of “Data Breaches” during the first period

Miscellaneous errors
- Incorrect delivery: when sensitive information reaches the wrong person;
- Incorrect publication: when non-public information is disclosed on a public web server;
- Missing or incorrect destruction of no longer needed personal data.

Web app attacks
Theft of access credentials and misuse of the web application.

Insider misuse
Abuse of the privileges granted to those who have obtained trust and therefore have access to sensitive data.

Crimeware
These are malware infections that are not associated with more specific classifications such as cyber. In any case they are attacks based on the concept of Command & Control.
To **prevent, manage** and **resolve** episodes of loss and/or destruction of personal data is possible:

- adopt a specific protocol to face the event;
- carry out periodic tests to check the validity of the protocol;
- obtain insurance coverage for any cases of data breach;
- keep a record of data breach cases;
- carry out investigations to identify the nature and extent of the breach.
The first few months of application of
The “Designated Subjects”

In addition to the already known roles as per the GDPR (i.e. Controller, Processors and DPOs) which are, each for his own part, responsible for the processing of personal data and surveillance of compliance with the requirements set forth by the GDPR, the Legislative Decree introduces the possibility for the Controller to appoint some peoples as “Designated subjects”.

These latter, in fact, are those who are assigned by the Controller or by the Processor, specific tasks within the organizational structure, with specific reference to the processing of personal data. They will no longer be recognized as internal processors but only as designated subjects.

They should be:

1. **Individuals** (not Entity)
2. **Part of the organizational structure** (an employee, a collaborator a Board Member, etc.)
3. **Formally appointed** by the Controller or the Processor
After an assessment aimed at verify the correctness of the two companies behaviors, the Authority has established that:

- up to 2 million promotional telephone calls were made in Vodafone’s interest and around 22 million text messages were sent without the interested parties having given their consent. These unsolicited commercial offers were addressed to current and potential customers, as well as to users who had changed telephone companies and also to users who had expressly requested to have their contacts deleted from the Vodafone databases.
- the Italian Guarantor has ordered Fastweb to pay € 600,000 for having conducted telemarketing campaigns without the consent of the persons contacted and for having adopted incorrect profiling of its customers (i.e. without first obtaining their informed consent and without having fully notified the Guarantor).

According to the **Italian Guarantor**, the new obligation of electronic invoicing - as from January 1st, 2019 extended also to relations between suppliers and between suppliers and consumers - presents "a high risk for the rights and freedoms of the interested parties, entailing a systematic, generalised and detailed processing of personal data on a large scale, potentially relating to every aspect of the daily life of the entire population, disproportionate to the pursued public interest, although legitimate".

The **Italian “Agenzia delle Entrate”** will only be able to store the fiscal data necessary for automated controls (e.g., inconsistencies between declared data and those available to the Agency), with the exception of the description of the good or service being invoiced.

The **Italian “Agenzia delle Entrate”** may file invoices only at the request of taxpayers who need to consult them.

The subjects who provide health services will not have to issue electronic invoices.

Further efforts are required to the Italian “Agenzia delle Entrate” to implement data encryption, minimize the data to be stored and comply with the obligations of transparency and fairness towards those data subjects.

A new Privacy Impact Assessment is planned, to be produced by the Agency by April 15th, 2019.
The CNIL has ordered Google LLC to pay a fine of €50 million, using for the first time in France the highest category of sanctions provided for in the GDPR.

According to the French Authority, essential information on the Android operating system (such as the purposes of data processing, data retention periods or categories of personal data used to personalize ads) "are excessively scattered among multiple documents, with buttons and links on which you need to click to access additional information", resulting to much complex.

The user is required to "take too many actions" to know how the collected information is actually used to customize certain services, including GPS tracking.

The CNIL has not considered sufficient generic pop-ups with which the user declares "I agree to Google’s Terms of Service".

In addition to the above, the French Guarantor has also found that in some cases it is not clear to the user that the conditions to be accepted are not necessary for the operation of the device but have only a "legitimate commercial interest".

In January 2019, the Washington Post reported that Facebook risks a record fine from the U.S. supervisory authorities - higher than the $22.5 billion already imposed in 2012.

The company is accused of violating binding agreements with the U.S. government in order to protect the privacy of users.

These agreements require Facebook to inform users and ask for their consent before data is shared with third parties in a different way from existing privacy settings.

A legally binding ordinance also requires Facebook to notify the Federal Trade Commission in cases where third parties misuse such information.

The same ordinance also prohibits Facebook from making misleading statements about its privacy practices and from carrying out external controls on the way in which data is used.
Data protection

According to the GDPR’ provisions, any transfer of personal data to a third country, including Japan, shall take place only when:

• the European Commission issued an adequacy decision, stating that the level of protection of personal data ensured by the third country is equal to that required by the GDPR;
• one of the appropriate safeguards listed by article 46 GDPR have been provided by the data importer (e.g. adopting binding corporate rules or standard data protection clauses);
• one of the specific situations listed in article 49 GDPR, that justify a derogation, exists (among other, obtaining a specific consent of the data subjects to transfer their personal data).

Also the “Japanese Act on Protection of Personal Information” (“APPI”) establishes similar restrictions to the transfer of personal data to foreign countries (i.e. including all the European Union Member States).

Since July 2017 the Japanese Government and the European Commission advanced a dialogue to promote higher standard of personal data protection. After a first joint statement on July 4, 2017, the last September 5, 2018, the EU and Japan started their respective procedures to the adoption of reciprocal adequacy decisions in order to consider, respectively, Japan and the EU Member States as having an adequate level of protection of personal data.

Finally the EU approved on January 23rd, 2019 the Adequacy Decision allowing personal data to flow freely between the two Countries on the basis of strong protection guarantees. In fact, before the Commission adopted its adequacy decision, Japan put in place additional safeguards to guarantee that data transferred from the EU enjoy protection guarantees in line with European standards.

Through this decision, Europeans’ data will benefit from high privacy standards when their data is transferred to Japan.

After two years from its entering into force, a first joint review will be carried out to assess the functioning of the framework. This will cover all aspects of the adequacy finding.
Data protection

The new GDPR also impacts significantly on the processing of personal data carried out in the context of employment relationships.

The EU Member may provide, by law or through collective agreements, specific rules to ensure the protection of rights with regard to the processing of personal data of employees in the context of employment relationships, in particular for the recruitment, execution of the employment contract, including fulfillment of the obligations established by law or collective agreements, management, planning and organization of work, equality and diversity at work, health and safety at work, protection of property of the employer or of the client and in order to guarantee the exercise and enjoyment, both on an individual or collective base, of all the rights and advantages connected to the job, as well as due to termination of the employment relationship.

These rules must include appropriate and specific measures aim at protect:

- human dignity;
- legitimate interests;
- the fundamental rights of data subjects, in particular regarding the transparency of data processing, the transfer of personal data within a business group or group of companies carrying out a common economic activity and workplace monitoring systems.

The GDPR allows the processing of sensitive data (personal data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, or union membership, genetic data, biometric data intended to identify a person, data relating to the health or sex life or sexual orientation of the person) even without the consent of the data subject when «processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law» or «processing is necessary to protect the vital interests of the data subject or of another natural person» or «processing is necessary for the establishment, exercise or defence of legal claims».
Data protection

The **Employer’s power of controlling its employees.**

This power represent a direct follow up of the general directive power of the Employer recognized to him from art. no. 2104 of the Italian Civil Code and which arises from the need to verify: (i) that the work of employees is carried out according to the methods indicated by the employer and that (ii) the company policies are respected (to protect the company’s assets and image against any theft or damage).

More in detail, art. 4 discipline the **conditions of legitimacy of controls** carried out by “audiovisual equipment and other control instruments”.

This provision could imply different aspect connected to the employees’ relationship, such an example:

- processing on personal data on Social Networks;
- monitoring of assigned Mobile Devices;
- use of information arisen from electronic badge or similar instruments used to identify the presence of the employees at work;
- use of GPS Systems;
- transfer of personal data outside the Company.

**Law no. 179/17** on reports of crimes or irregularities in the context of an employment relationship (the so-called "Whistleblowing") has been inserted into the new legal framework of personal data protection. In the construction of the Whistleblowing process it will be fundamental, therefore, to pay attention to the regulatory constraints on the protection of personal data.

It is important to recall the recommendation provided in July 2016 by the «European Data Protection Supervisor» and contained in the "Guidelines on processing personal information within whistleblowing procedures" for the creation of whistleblowing schemes:

- **adequate guarantees on the confidentiality** of the information received and on the protection of the identity of the reporters and of all the other persons involved;
- the correct application of the principle of **minimization of data processing**;
- clarify what is meant by "personal information" and who the persons concerned are in order to determine their right to information, access and correction;
- data **retention periods proportionate** to each individual reporting case;
- organizational, safety and techniques measures based on adequate risk assessment.
**Data protection**

- **As Is & Gap Analysis** considering the new European Regulation, including the assessment aimed at identifying, among other:
  - types of processed data, purposes and methods of processing;
  - new requirements required to Data Owner and Data Processor.

- **Presentation to the Board / other Committees / top management of the assessment results.**

- **Support to DPO, Internal Audit and Compliance Functions** in carrying out the relevant monitoring controls related to the new European Regulation

- **Indipendent Audit** on the approach adopted by the Company.

- **Design of operating model** within the perspective of “privacy by design” and “privacy by default”;
- **Design of Codes of Conduct**;
- **Design of Internal procedures**;
- **Design of Appointment documentation (DPO, Data Owner and Data Processor, etc.)**.

- **DPO activities’ definition**;
- **Register management**;
- **Privacy impact assessment**;

- **Data Owner & Data Processor contracts readiness/revision**;
- **Training and information** (i.e. newsletter);
- **Support for the relationship with the Relevant Supervisor**.
The PwC Network entities have skills, experiences and resources that allow a global geographical coverage and a multidisciplinary approach.

- Our legal experts cover wide territories with specific skills in data privacy matters
- Our Risk&Compliance experts are able to support Organizations in all aspects related to the analysis, design, implementation and monitoring of compliance requirements.
- Our IT experts have relevant professional certifications (ITIL, ISO270001, CISA, CRISK, CGEIT, CISM), having also knowledge and expertise in the emerging technologies and we are currently positioned as Leader in the "Forrester Wave for InfoSec Consulting Services".
What is Cybersecurity?

Ability of an organization to protect its people, data, systems and reputation in the «cyberspace» (an online world where people, data and systems are interconnected through technology)*

Preservation of confidentiality, integrity and availability of information in the Cyberspace. The «cyberspace» is a complex environment resulting from interaction of people, software and service on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.

(*) Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit organisation with a Membership comprising many of the world’s leading organisations featured on the Fortune 500 and Forbes 2000 lists.

(**) The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST’s mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
Cybersecurity: why it is important?

Cyber attacks are growing and they increase data loss

Source: http://informationisbeautiful.net
Loss: more than 30,000 records
(updated til 15 October 2018)
CEOs and investors are both concerned about cyber threats

A company’s ability to **build** and **maintain trust** with its stakeholders is important; some say it gives the company its licence to operate.

Trust can be achieved by **investing more in cyber security defences** and being transparent about how they use and store customer data.

Technological advancements are in the news on a regular basis, so it is no surprise that **investment professionals’ and CEOs’ concerns** about the speed of technological change and **cyber threats** have increased.

Source: PwC Global Investors Survey 2018
Cybersecurity is a priority

Cybersecurity breaches erode companies’ share prices permanently and have resulted in **$148 per lost or stolen record**.

Companies are becoming digital and current approaches to cyber risk management must **evolve from subjective, checklist and compliance driven methods to data-driven risk models**.

The role of Boards in cyber risk oversight is increased and is driving demand for better methods to measure and articulate business and economic impacts of cyber risks.
A key regulatory focus

The NIS Directive (see EU 2016/1148) is the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU. The NIS directive was adopted in 2016 and subsequently, because it is an EU directive, every EU member state has started to adopt national legislation, which follows or ‘transposes’ the directive.

The NIS Directive was adopted in Italy through Decreto Legislativo n. 65 (18 May 2018) and it focuses on two main points:

- Adoption of technical and organizational measures to prevent and minimize security incidents impacts on critical market operators, in order to grant service continuity;
- Implementation of a notification process to the competent national NIS authority for timely report incidents impacting continuity of critical services.

Non compliant entities are subject to administrative sanctions and reputational damage.

The accelerated pace of regulatory enforcement around cybersecurity and privacy highlights the changing expectations for organizations to establish demonstrable cybersecurity risk management programs.

April 2015
U.S. Securities and Exchange Commission (SEC) issued guidance regarding disclosure obligations relating to cybersecurity risks and incidents

April 2016
European Union (EU) adopts the General Data Protection Rule (GDPR) impacting cybersecurity and privacy for global businesses

February 2017
New York Department of Financial Services (NY DFS) signed into law cybersecurity regulations impacting financial services institutions subject to NY DFS regulation.

April 2017
AICPA issued a reporting framework to develop a consistent, profession-wide approach to performing attestation engagements related to cybersecurity

May 2017
U.S. Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity issued

June 2017
China Cybersecurity Law effective, impacting global businesses

2017 and beyond
There will be continued interest in cybersecurity regulation and enforcement with a possibility of increased oversight (e.g. Department of Defense cybersecurity requirements - DFARS)
Cybersecurity core focus areas

To exercise their fiduciary duty, boards need comfort that they have a "defensible" cybersecurity risk management program in place.

- Effectiveness of cybersecurity governance and oversight
- Protection of networks and customer information
- Identification and assessment of cybersecurity risks and threats
- Management of cyber risks associated with vendors and other third parties
- Detection and prevention of unauthorized activity
- Response to data breaches and minimization of business disruption

Is the business resilient to a cyber attack?

Which threats should we be most concerned about?

Could a cyber incident impact our business?

Are there gaps in our cybersecurity capabilities?

How much risk are we willing to take?

Are we spending in the right areas?
How to approach Cyber & regulatory risks: NIST framework

The NIST Cybersecurity Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk, to help organizations to evaluate and improve their ability to prevent, identify and respond to cyber attacks.

Maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident, including Recovery Planning and Controls Improvement.

Take action regarding a detected cybersecurity incident, including Response Planning, Communications and Mitigations.

Identify the occurrence of a cybersecurity event through appropriate activities (i.e. Continuous Monitoring and Detection Processes).

Understand the business environment and the resources/assets that support critical functions; execute Risk Assessment; define Risk Management Strategy.

Ensure delivery of critical services with regards to the identified risks through appropriate safeguards (i.e. Identity Management and Access Control, Awareness and Training and Data Security).
How can PwC help?

- Implementation and evaluation of Information Security systems (i.e. ISO27001, NIST, ISF)
- Cybersecurity awareness (i.e. Game of Threats)
- Service Organization Controls for cybersecurity
- Analysis of insurance coverage about cyber security
- Swift Customer Security Program (CSP)
- Dark-net researches
Contact details

Giuseppe Garzillo
Risk Assurance Services
Partner
Mobile: +39 348 2504033
giuseppe.garzillo@pwc.com

Dino Ponghetti
Risk Assurance Services
Associate Partner
Mobile: +39 348 1505207
dino.ponghetti@pwc.com

Simona Bellavia
Risk Assurance Services
Director
Mobile: +39 348 1505622
simona.bellavia@pwc.com

Federico Dolzani
Risk Assurance Services
Senior Manager
Mobile: +39 334 6550821
federico.dolzani@pwc.com

Marco Montanini
Risk Assurance Services
Director
Mobile: +39 348 0703149
marco.montanini@pwc.com

Emanuele Motta
Risk Assurance Services
Senior Manager
Mobile: +39 347 9402379
emanuele.x.motta@pwc.com
**Contact details of Japanese Business Network**

**Simone Marchiò**

Executive Director  
M&A Tax  
Leader for the Italian Japanese Business Network

*Mobile: +39 3471072824  
Email: simone.marchio@pwc.com*

Simone is an Executive Director of the Tax M&A department. He is also the coordinator of the Japan Business Network (JBN) activities in the Tax and Legal Department of PwC Italy.

Simone has 13 years experience in tax, accounting and corporate consulting to medium-large size firms of multinational groups. He is author of articles on Italian and international tax magazines.

Simone is specialized in M&A. Simone has experience in advising domestic and multinational companies on domestic and international tax matters, corporate reorganization, tax due diligence and he is an internal auditor of some multinational companies.

**Eva Sorgato**

Senior Manager  
M&A TAX  
Japanese Business Network

*Mobile: +39 342 5919667  
Email: eva.sorgato@pwc.com*

Eva has spent the last 9 years working with PwC M&A tax practice in Milan, focusing on M&A projects (tax due diligence, international tax structuring, tax modelling, SPA tax assistance) for both corporate clients and institutional investors.

Her PwC experience includes a secondment with the OECD in Paris from 2011 to 2013, focusing on tax planning and tax transparency areas.

She graduated in Business Law at Bocconi University in Milan in 2009 and she was admitted in 2013 to the Order of Certified Public Accountants ("Ordine dei Dottori Commercialisti") in Milan.

[Language]  
Italian, English

[Language]  
Italian, English, French
Contact details of Japanese Business Network

Daniela Bagarella
Manager
PS Labour Law

- **Mobile:** +39 348 5600288
- **Email:** Daniela.bagarella@pwc.com

Daniela is a Manager of People Services Department based in Milan and has accrued more than 8 years of professional experience in labor matters during which she gained a wide experience in the management of a variety of HR related matters.

Daniela has accrued her experience in the management of several labour matters and related services, including: (i) management of employment relationships; (ii) labor law issues in the context of corporate reorganization and restructuring operations; (iii) collective / individual dismissal procedures; (iv) company transfer procedures; (v) judicial litigation with employees and with public authorities; (vi) due diligence on the buyer and seller side.

Daniela also gained a wide experience in the management of regulatory compliance activities, especially with reference to Health & Safety at Work and compliance with European Legislation on the processing of Personal Data (GDPR).

- **Language**
  - Italian (native), English (fluent) and French.

Ai Hasegawa
Manager
Japan Business Network

- **Mobile:** +39 3443438487
- **Email:** ai.i.hasegawa@pwc.com

Ai joined PwC Mexico in January 2016 as a business development at Japanese Business Network (JBN) and supported Japanese companies for assurance, tax and advisory services. She got transferred to PwC Milan in March 2018 in order to build JBN in PwC Italy.

She has working experiences in a wide range of field such as manufacturing companies in energy sector, trading companies in automotive sector and consulting companies.

- **Language**
  - Japanese, English, Spanish
Thank you