POLITECNICO MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET digital innovation

Siete pronti per il GDPR?

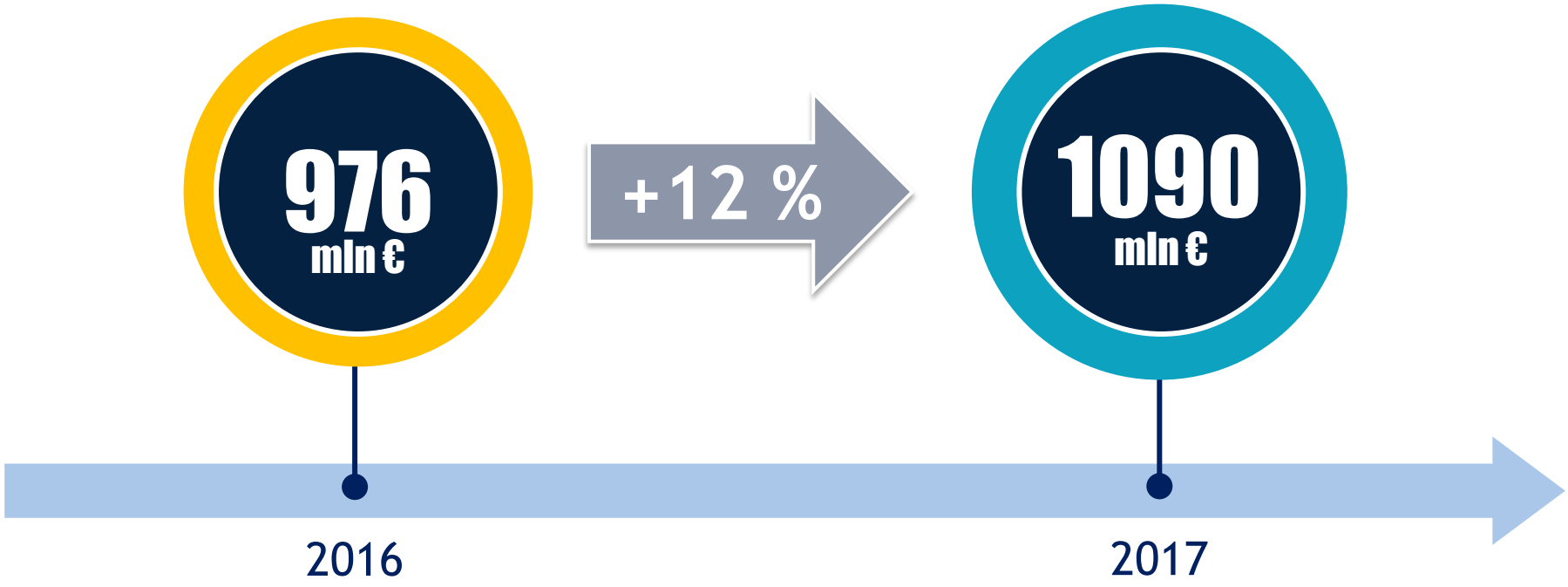
Inquadramento generale del GDPR

Avv. Annamaria Italiano

3 maggio 2018

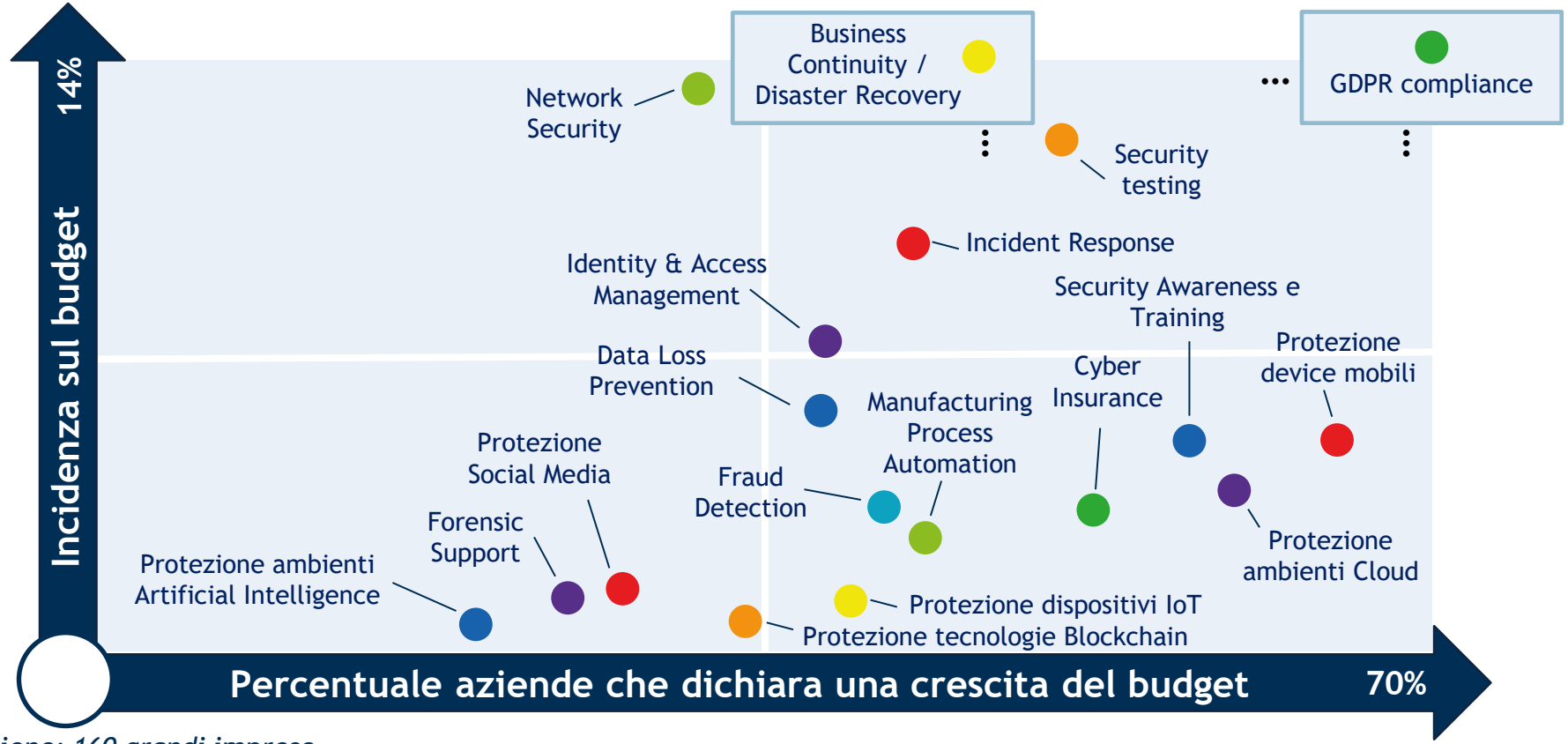
Il mercato Information Security 2017

OSSERVATORI.NET digital innovation



Campione: 1107 organizzazioni italiane

La scomposizione del mercato Information Security



Campione: 160 grandi imprese

Le principali motivazioni di spesa delle PMI

OSSERVATORI.NET digital innovation

TUTELA DEI DATI DEI CLIENTI

45%

ADEGUAMENTO ALLE NORMATIVE

19%

ATTACCHI INFORMATICI SUBITI

11%

TUTELA DELLA PROPRIETÀ INTELLETTUALE

8%

PROTEZIONE DI AMBITI APPLICATIVI CORE

6%

Dati ottenuti tramite un'elaborazione statistica di un campione di 947 micro, piccole e medie imprese (addetti compresi tra 2 e 249)

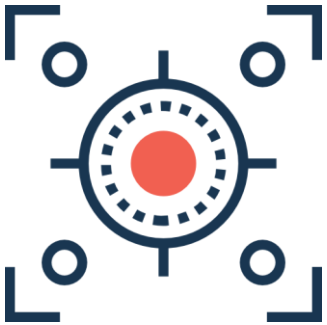
L’iter normativo

RIFORMA EUROPEA PRIVACY

Il percorso legislativo di adozione del GDPR è iniziato il **4 novembre 2010**, quando la Commissione europea ha elaborato una proposta di riforma della normativa in materia di protezione dei dati personali

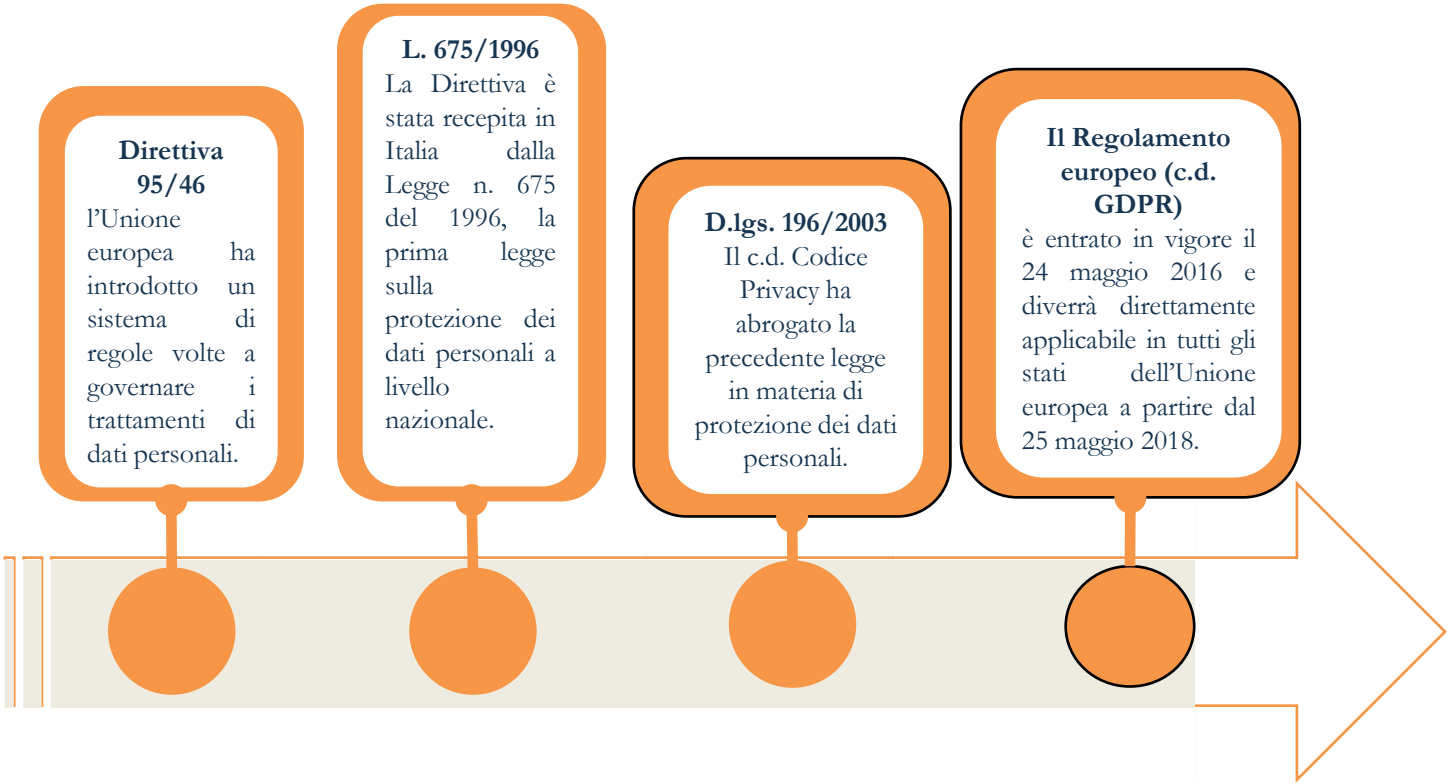
PRINCIPALI OBIETTIVI

ADEGUARE la NORMATIVA (risalente ormai a 20 anni fa…) alle **NUOVE TECNOLOGIE** (Social Network, Cloud Computing, App web e mobile, Bid Data, etc)



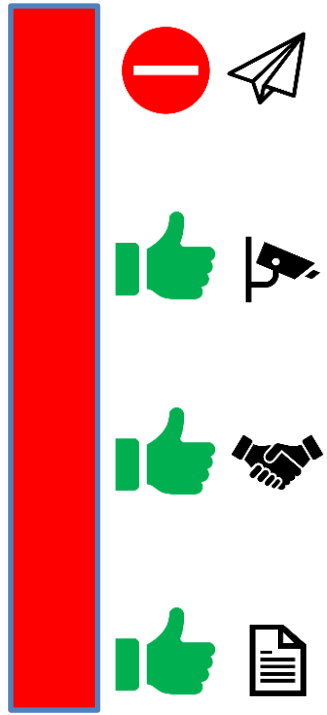
ARMONIZZARE ed **UNIFORMARE** la NORMATIVA a livello europeo, creando un quadro legislativo comune in modo da evitare di far fronte a normative differenti in ciascuno stato membro

EVOLUZIONE NORMATIVA



Cosa accade a maggio 2018?

Autorizzazioni Generali Autorità Garante[1]	**IN VIGORE, DECADONO il 24 maggio 2018**
Provvedimenti Autorità Garante	**NON DECADONO** fino a quando non verranno modificati, sostituiti, abrogati
Accordi internazionali su trasferimento dati	**NON DECADONO** fino a quando non verranno modificati, sostituiti, abrogati
Decisioni Commissione UE	**NON DECADONO** fino a quando non verranno modificate, sostituite, abrogate



[1] I provvedimenti che consentono a varie categorie di titolari di trattare dati sensibili e giudiziari per gli scopi specificati senza dover chiedere singolarmente un'apposita autorizzazione al Garante.

Cosa cambia marginalmente

e

quali sono le novità del GDPR

Cosa NON cambia o varia marginalmente nel Regolamento

- Definizione di dato personale
- Definizione di trattamento
- Soggetti che effettuano il trattamento (salvo DPO)
- Principi relativi al trattamento di dati
- Liceità del trattamento
- Informativa
- Consenso
- Protezione delle sole persone fisiche

Le novità introdotte dal GDPR

- Accountability del titolare
- Nuovi doveri del titolare:
  - Registro dei trattamenti
  - DP by design e by default,
  - DP impact assessment
- Sicurezza:
  - Eliminazione misure minime
  - Notifica data breach
- Responsabilità solidale di titolare e responsabile
- DPO
- Nuovi diritti degli interessati:
  - Tempo di conservazione
  - Portabilità
  - Oblio
- Certificazione dei trattamenti
- Entità delle sanzioni

IMPLICAZIONE DELL'ACCOUNTABILITY PER I TITOLARI

La **maggiore discrezionalità** per i TITOLARI di **DECIDERE** le **MODALITÀ** attraverso le quali conformarsi alle sue disposizioni è gravata dall'ONERE di essere IN GRADO DI DIMOSTRARE le **RAGIONI** che hanno portato a tali decisioni e le **MOTIVAZIONI** alla base delle scelte

Sarà per esempio necessario essere in grado di documentare il processo che ha portato alla valutazione di un determinato rischio in materia di sicurezza, alla decisione di notificare o meno agli interessati un «data breach», di aver attuato in relazione ad un nuovo trattamento le necessarie valutazioni legate alla privacy «by design»

OBBLIGHI IN CAPO AL TITOLARE

PRIVACY BY DESIGN

Realizzare qualsiasi progetto, servizio o sistema (sito web, software, soluzione IT, ambiente di lavoro, etc.) considerando la riservatezza e protezione dei dati personali sin dalla progettazione, utilizzando tecniche quali la minimizzazione e pseudonimizzazione

PRIVACY BY DEFAULT

Trattare di default solo i dati necessari («**minimizzazione**» dei dati già in fase di raccolta)

MISURE DI SICUREZZA ADEGUATE (ART. 32, CO. 1)

NON sono più previste **MISURE MINIME** come quelle indicate tassativamente e «tipizzate» nell'Allegato B D.Lgs. 196/03

TITOLARE
CONTROLLER

RESPONSABILE
PROCESSOR

Mettono in atto

Misure **TECNICHE** ed **ORGANIZZATIVE** **adeguate per garantire un livello di sicurezza** adeguato al rischio…

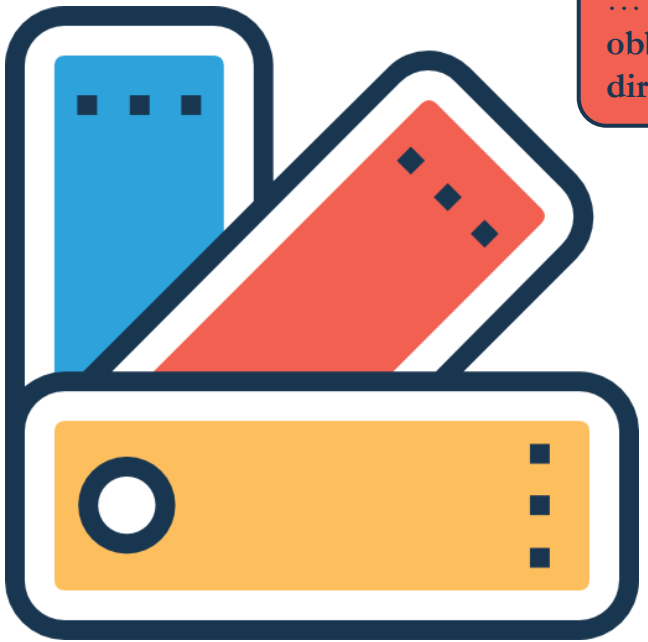
… tenuto conto di:

STATO DELL'ARTE e dei **COSTI DI ATTUAZIONE**, nonché **NATURA, AMBITO, CONTESTO, FINALITA', RISCHI**

Cambia il rapporto fra Titolare e Fornitori

NUOVE RESPONSABILITÀ PER I FORNITORI (RESPONSABILI)

Il **responsabile** risponde non solo se **ha agito in modo difforme o contrario rispetto alle** legittime **istruzioni del titolare…**



… ma anche se **non ha adempiuto gli obblighi del regolamento specificatamente diretti ai responsabili**

RESPONSABILITÀ SOLIDALE

Qualora più titolari o responsabili oppure entrambi siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni **titolare** o **responsabile** è responsabile **in solido** per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato

Nuovi ruoli: il DPO

DATA PROTECTION OFFICER (C.D. DPO)

https://edps.europa.eu/data-protection/our-work/subjects/data-protection-officer_en

Il GDPR ha introdotto la nuova figura del Data Protection Officer (c.d. DPO), disciplinandola agli artt.37-39

Il DPO svolge uno ruolo fondamentale all'interno del nuovo sistema di *governance* dei dati

COMPITI DEL DPO

FUNZIONI

CONSULENZA
informare e consigliare il Data Controller, il Data Processor e i dipendenti in merito agli obblighi del GDPR

COOPERAZIONE
con l'Autorità di controllo

VIGILANZA
sorvegliare l'osservanza del GDPR

FORNIRE UN PARERE
in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento

CONTATTO
per l'Autorità di controllo e gli interessati

DPO: OBBLIGATORIETÀ

QUANDO È NECESSARIO NOMINARLO?

Il trattamento sia effettuato da un'**autorità pubblica**

Il "*core business*" dell'azienda consista nel trattamento "**su larga scala**" **di dati "sensibili" e "giudiziari".**

(LARGA SCALA: Numero di persone interessate (numero specifico o percentuale della popolazione pertinente); Volume di dati; Durata delle operazioni di trattamento; Estensione geografica delle attività.)

Il "*core business*" dell'azienda consista in attività che richiedono il **monitoraggio regolare e sistematico di dati "su larga scala".**

(Monitoraggio regolare: Continuo, ripetuto, svolto costantemente/ripetutamente; **Monitoraggio sistematico:** Preorganizzato, parte di una strategia ben precisa)

INFINE… LE SANZIONI

L'ammenda amministrativa può arrivare fino **a 10.000.000 EUR o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente** se superiore, in caso, tra l'altro, di **violazione delle disposizioni relative agli obblighi del titolare del trattamento e del responsabile del trattamento**

L'ammenda amministrativa può arrivare fino **a 20.000.000 EUR o per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente** se superiore, in caso, tra l'altro, di **violazione delle disposizioni relative ai principi base del trattamento e ai diritti degli interessati**.

La mancata comunicazione di una violazione potrebbe evidenziare l'assenza di misure di sicurezza o un'inadeguatezza delle stesse. In tal caso, l'autorità di vigilanza oltre alla possibilità di emettere sanzioni per mancata comunicazione (ex art. 33 e 34) può anche sanzionare l'assenza di misure (adeguate) di sicurezza (ex articolo 32), in quanto trattasi di due violazioni distinte.

IMPLICAZIONI PER LE AZIENDE

Predisporre un **SISTEMA DI GESTIONE DELLA DATA PROTECTION**

1. Considerare la privacy sin dalla fase di progettazione

4. Formalizzare la documentazione di adeguamento ai singoli obblighi normativi

2. Attribuire RUOLI e RESPONSABILITÀ in materia di data protection; formalizzare un preciso **organigramma privacy interno** che definisca "chi fa cosa", coerentemente alle mansioni azienda

5. Implementare **meccanismi di controllo interno** per verificare l'effettiva applicazione delle misure adottare e adeguate politiche di informazione aziendale

3. Prevedere regolamenti e procedure per la gestione della data protection

6. Monitorare le misure ed aggiornale se necessario

GRAZIE PER L'ATTENZIONE!

Annamaria Italiano

annamaria.italiano@p4i.it