CONVEGNO Reg. UE 679/2016

Quality Management S.r.l.

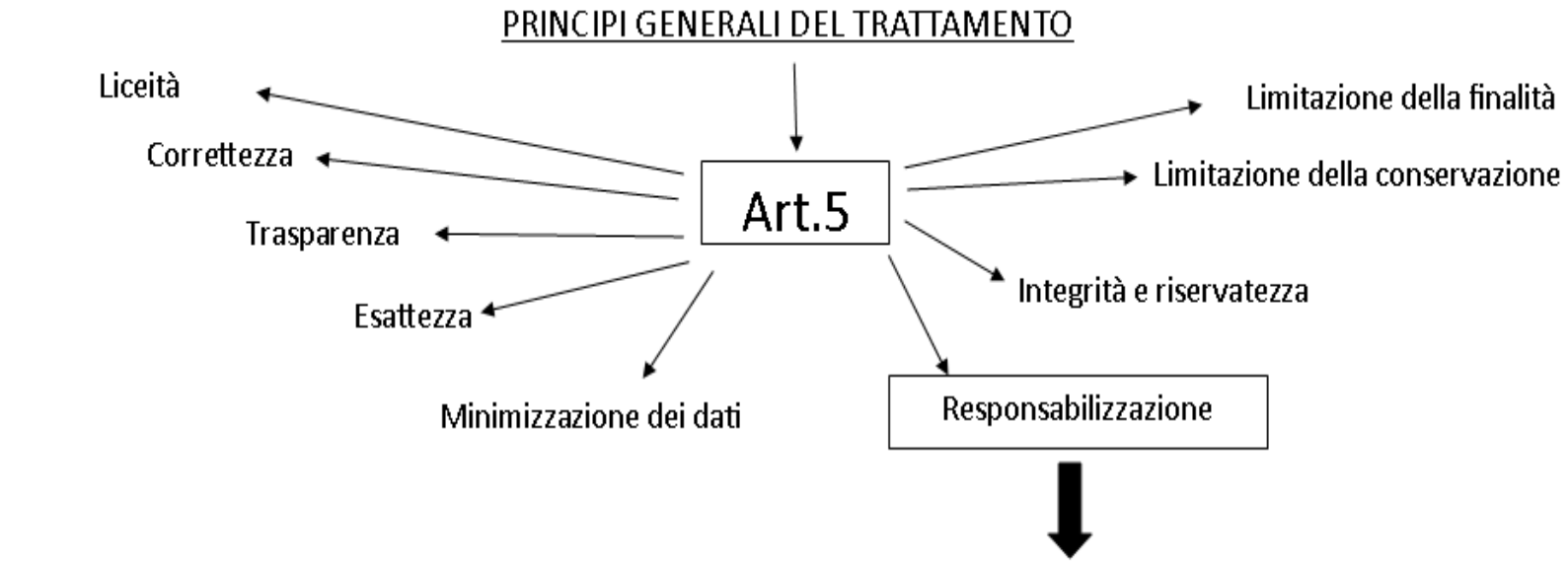
- COLLE V.E. – 04 maggio 2018 -

DataProtection

Relatore Dott. **Giampaolo Rachini**

GDPR: Principali ambiti di intervento

PERSONE:	PROCESSI:	TECNOLOGIE:
• Aggiornamento e comunicazione delle nuove policy aziendali sulla privacy • Formazione sulla nuova disciplina privacy europea per il personale • Formazione mirata per ambiti aziendali specifici (es. Area commerciale, HR, ecc..) • Misure integrative di formazione e sensibilizzazione (es. Privacy Day, piani di comunicazione, ecc..)	• Due Diligence & Gap Analysis • Revisione Incarichi • Revisione informative e consensi • Adozione nuove misure organizzative di sicurezza • Privacy Impact Assessment • Definizione modelli registri dei trattamenti (OBBLIGATORIO) • Procedure: Data Breach, Privacy by Design & by Default, esercizio diritti interessato (es. portabilità, oblio, ecc..)	• Assessment tecnologico delle misure di sicurezza • Adozione nuove misure tecniche di sicurezza • Adozione di strumenti tecnologici a supporto dei nuovi adempimenti



Accountability: devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati

Maggior attenzione al CONSENSO (art.7)...

L'Art.7 enuncia che il trattamento sia basato sul consenso ed il titolare del trattamento dev'essere in grado di dimostrarlo nei rispetti dell'interessato;

Il consenso dev'essere libero, chiaro e distinguibile dalle altre materie, nonché comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

Il trattamento dei dati è lecito ove l'interessato abbia più di 16 anni, nel caso contrario è necessario il consenso prestato o autorizzato dal titolare della responsabilità genitoriale. (Art.8)

PRIVACY

2 aziende italiane su **3** hanno le idee confuse

Potranno arrivare fino a **20 milioni di euro** o al **4% del fatturato annuo** dei trasgressori, queste sono le sanzioni previste dal Regolamento UE 2016/679 che sarà applicabile dal **25 Maggio 2018**.

Alcuni Dati:

- Il **75%** delle imprese si doterà di un Referente Interno Privacy

- Il **32%** delle imprese non sa ancora se rientra nell'obbligo di nomina di un DPO
- Il **72%** delle imprese non ha nominato nessuno come DPO

- Il **22%** ha nominato il DPO all'interno dell'area Information Technology, esponendosi quindi a rischi di sanzioni, art.38 del Regolamento:

«…il titolare debba assicurarsi che i compiti svolti dal DPO non diano adito a un conflitto di interessi…»

Le figure della vecchia e della nuova PRIVACY

D. Lgs 196/2003	GDPR
• Titolare del Trattamento	Data Controller
• Responsabile del Trattamento	Data Processor
• Incaricati del Trattamento	Non prevista, ma nemmeno esclusa
	New entry:
	• **Joint Controller (Contitolare)**
	• **DPO**

REGOLAMENTO PRIVACY UE: pro e contro del nuovo sistema sanzionatorio

D.Lgs. 196/2003

- Il Codice della privacy italiano prevede che ad un illecito commesso corrisponda necessariamente la sanzione pecuniaria

GDPR

- Il Regolamento Europeo, per le ipotesi di minore gravità, **ammette l'alternativa tra sanzione pecuniaria e ammonimento** (Art.58)

Con il GDPR si potrà valutare lo stato **soggettivo** e, quindi, tenere conto del fatto che il titolare del trattamento, ad esempio, è una piccola o media impresa.

I parametri per l'applicazione delle sanzioni sono 11 contro i soli 4 previsti dall'attuale Codice Privcy.

Le indicazioni dei **Garanti Europei** per tutelare la privacy dei lavoratori

- I Garanti hanno ricordato che **ogni lavoratore**, indipendentemente dal tipo di contratto a lui applicato, ha **diritto al rispetto della vita privata, della sua libertà e dignità**
- Il lavoratore dev'essere **adeguatamente informato** sulle modalità di trattamento dei dati personali in maniera chiara, semplice ed esaustiva, soprattutto quando sono previste forme di controllo del lavoratore (ovviamente a norma di legge)
- E' possibile introdurre strumenti e tecnologie, come quelle per l'analisi del traffico, per ridurre i rischi di attacchi informatici e la diffusione di informazioni riservate, ma **NON** si può spiare la posta dei dipendenti o la loro navigazione internet

Controlli sulle **Email** legittimi solo se il lavoratore è informato!

1. Innanzitutto il lavoratore dev'essere informato del **controllo**, della sua **natura** e della **ricorrenza** anticipatamente
2. Devono sussistere **sufficienti ragioni** per realizzarlo
3. Il datore deve usare le modalità meno intrusive possibili per realizzare i controlli, limitandoli nel tempo e nel contenuto

VIDEOSORVEGLIANZA

A rischio privacy, servono competenze e nuove regole

Come tutti i dispositivi connessi al web (IoT: *Internet of Things*), implicano anch'esse delle criticità e delle vulnerabilità che sempre più spesso vengono sfruttate da malintenzionati per spiare gli stessi proprietari che le hanno installate

NEL 2018 SARANNO QUASI 1 MILIARDO

Non è tutto, per evitare gravi violazioni della privacy di cittadini e lavoratori, è necessario avvalersi di professionisti sia in campo tecnico che nel campo giuridico

Ricordiamo, inoltre, l'ultimo provvedimento generale in materia di videosorveglianza emesso dal Garante è del 2010 e si attendono modifiche per il 2018.

Per questo dobbiamo essere pronti!!!!!!!!!!!!!!!!!!!!

EUROBAROMETRO

Gli europei vogliono più privacy online…un po' di dati
Cos'è MOLTO IMPORTANTE e per CHI:

- La protezione all'accesso per foto, calendario, contatti e altri dati (**78%** degli **europei** e **italiani**);
- Confidenzialità di email e messaggi (**72% europei** – **75% italiani**);
- Permesso ai cookies (**56% europei** – **67% italiani**)
- Che messaggi chat e mail siano criptati (**65% europei** – **69% italiani**)

Purtroppo solo il 40% degli **italiani**(contro il 60% degli europei) hanno modificato le impostazioni privacy nel loro browser
Ed in Italia scendiamo sotto il 30% di persone che si proteggono tramite software dedicati

GLI EUROPEI VOGLIONO PIU' PRIVACY

La revisione della direttiva sulla Privacy è arrivata a fine Gennaio e comporta alcune modifiche, facciamo un esempio:

- ***È il browser stesso (Chrome, Firefox, Explorer, etc.) a chiedere all'utente che tipo di tutela della privacy vuole, offrendo più profili di protezione…alto, medio o basso.***
- ***Whatsapp sta introducendo l'obbligo dell'età minima a 16 anni per l'utilizzo del social.***

Questo dimostra come l'imminente Regolamento trasformerà la privacy tramite una

rivoluzione totale!!

CASE STUDY: Facebook I

Il Garante della privacy spagnolo ha multato Faceboook per 1,2 milioni di euro per non aver impedito agli inserzionisti pubblicitari di accedere ai dati dei propri utenti.

Facebook così ha raccolto dati su *ideologia, sesso, religione, gusti personali e sulla navigazione, etc.,* senza **INFORMARE CHIARAMENTE** gli utenti sull'utilizzo e lo scopo della raccolta.

CASE STUDY: WhatsApp

3 milioni di euro per aver **INDOTTO** gli utenti ad **ACCETTARE INTEGRALMENTE** i nuovi termini di utilizzo, inducendo i nuovi iscritti a ritenere che *sarebbe stato, altrimenti, impossibile proseguire nell'uso dell'applicazione*, qualora **NON AVESSERO ACCETTATO LA CONDIVISIONE DEI LORO DATI PERSONALI CON FACEBOOK**

…e ancora (sempre facebook)…

CASE STUDY: Facebook II

Il Garante della privacy francese ha multato Facebook al pagamento di 150mila euro per **NON AVER INFORMATO IN MODO ADEGUATO GLI UTENTI IN MERITO ALLE MODALITÀ E AGLI SCOPI DEL TRATTAMENTO EFFETTUATO SUI LORO DATI PERSONALI** e per aver proposto pubblicità mirata in assenza di una base legale che lo consentisse

DATA BREACH

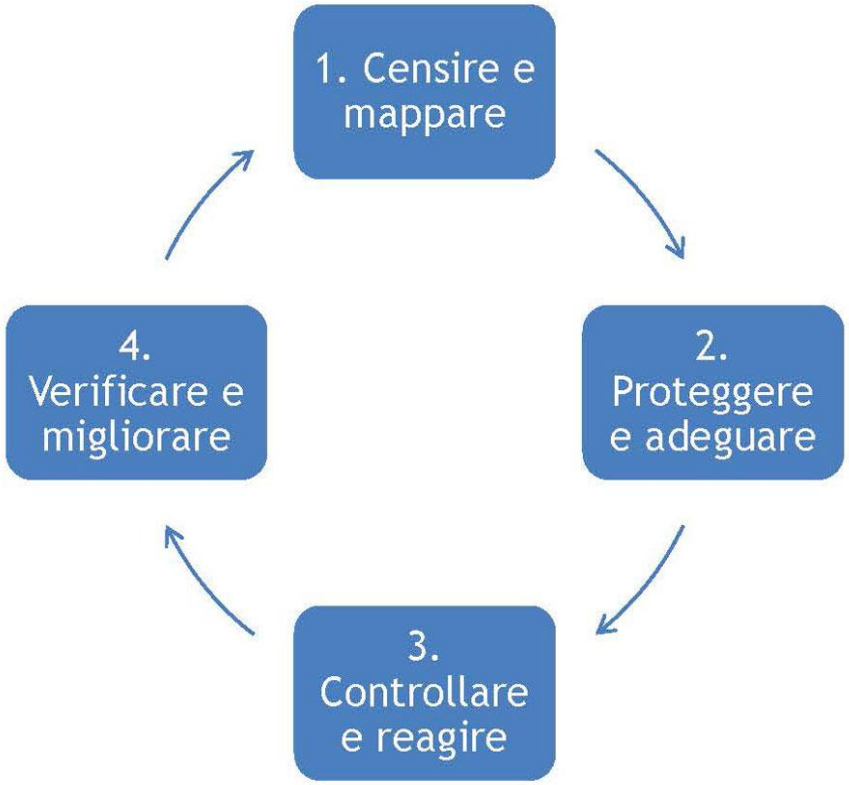
ALLARME CYBERSECURITY E PRIVACY A RISCHIO PER LE AZIENDE

Potrà sembrare incredibile, ma **bastano 20 euro e qualche ora di lavoro** di una persona con conoscenze di programmazione di base per **trasformare una semplice chiavetta USB in un potente strumento di «hacking»** in grado di infettare le reti informatiche di un'azienda con un malware.

Ricordiamo gli **oltre 450 milioni di password e indirizzi email** trafugati con il leak **Antipublic** e il devastante ramsomware **Wannacry**, che colpì più di **200mila** computer per prendere in ostaggio i dati di privati e aziende (quest'ultimo bloccato, per pura fortuna, da un ragazzo britannico di 22 anni)

Non c'è tregua per le aziende che arrancano per difendersi dalle minacce informatiche

COSA FACCIAMO PER LE AZIENDE



Dato personale (PII Personal Identifiable Information) = qualunque dato relativo e associato (o associabile) ad una persona fisica

Interessato (data subject) del trattamento = persona fisica a cui si riferiscono i dati personali, o meglio, il proprietario dei suoi dati

Titolare del trattamento (data controller) = soggetto giuridico che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali e decide quali categorie di dati personali devono essere raccolte

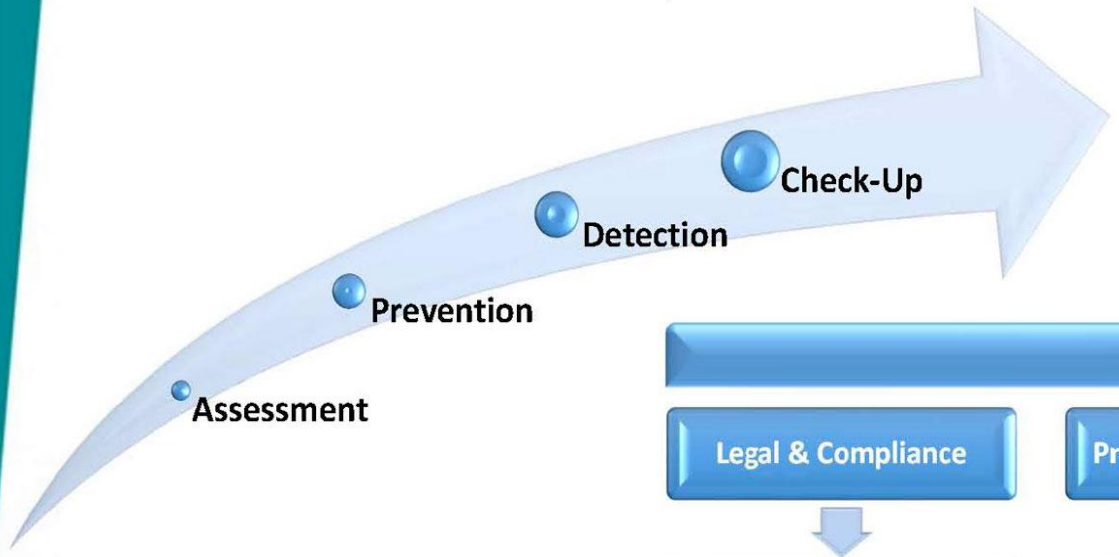
Responsabile del trattamento (data processor) = la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento. Il titolare del trattamento, quindi, nomina uno o più responsabili.

Quality Management S.r.l.

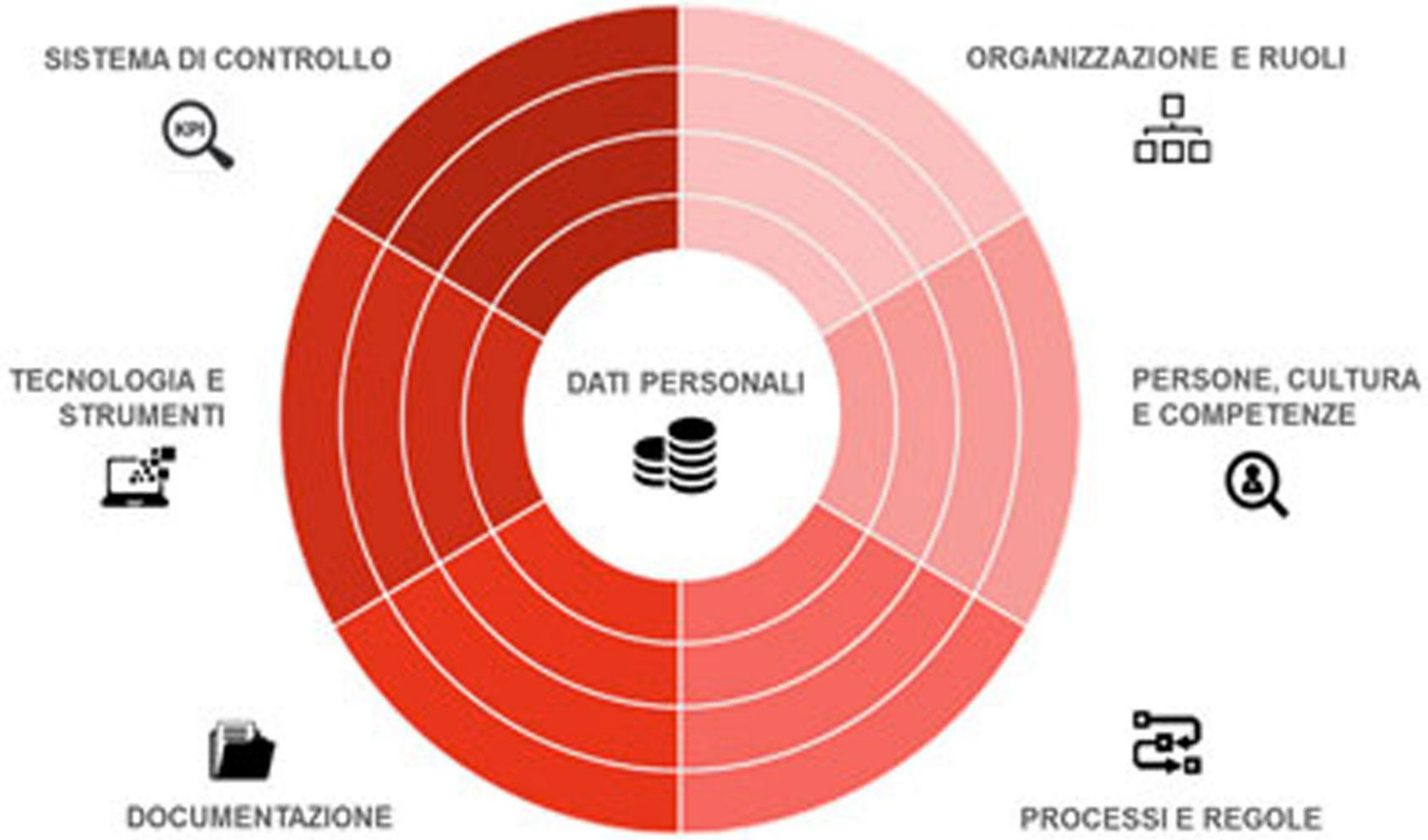
GDPR: Check-Up Periodico

"Monitoraggio e mantenimento degli standard"

Per ogni area, pianifichiamo un check-up degli standard raggiunti,
adeguando, ***mantenendo***, ***integrando*** laddove necessario e realizzando un piano di
miglioramento continuo nel tempo



MODELLO DI FUNZIONAMENTO DELLA DATA PROTECTION



GRAZIE PER L'ATTENZIONE