Enrico Magalini
Verona 09.05.2018

GDPR

Agenda

- Privacy: cosa è cambiato in 14 anni
- Dati, Reputazione diritti e libertà personali
- Concetto di Accountability (responsabilità) e proattività
- Nuovo approccio metodologico e concetto di rischio
- Nuova figura del DPO e Registro del trattamento
- Azioni concrete (formare, documentare, controllare)

Regolamentazione privacy pre 25 maggio

Le leggi sulla privacy in Italia sono:

- **Legge n. 675 del 31 dicembre 1996**

  Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali

poi abrogata e sostituita da:

- **Decreto Legislativo 30 giugno 2003, n. 196**

  Codice in materia di protezione dei dati personali

  Attualmente in vigore

Dopo 14 anni…

- Esplosione Social Media
- (Web) Marketing spinto
- Raccolta dati di ogni genere
- Big Data
- Cambridge Analitica
- Esteso impiego del Cloud
- …

Informazioni riservate pubblicate

Il 28% degli internauti condivide on line informazioni riservate per errore

Conseguenze:

- perdita di amici (20%)
- **atti di bullismo (17%)**
- perdite finanziarie (15%)
- fine di una relazione (13%)
- **perdita del posto di lavoro (13%)**

Protezione dei dati personali

- **Il legislatore riconosce la privacy come diritto fondamentale**
- Il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 nasce come *risposta* al diritto fondamentale della privacy
- **Rispettarne i diritti e le libertà fondamentali**

Agenda

- Privacy: cosa è cambiato in 14 anni
- Dati, Reputazione diritti e libertà personali
- Concetto di Accountability (responsabilità) e proattività
- Nuovo approccio metodologico e concetto di rischio
- Nuova figura del DPO e Registro del trattamento
- Azioni concrete (formare, documentare, controllare)

Dato personale e trattamento

- **dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile
- **interessato**: la persona fisica oggetto del trattamento
- **trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali

Esempi di dati

- Anagrafica completa
- Dati sanitari
- Il titolare della licenza di un PC con nome, cognome, codice fiscale…

Qualità del dato da preservare

Riservatezza →	Riservatezza: chi può accedere? I documenti sono protetti?
Integrità →	Integrità: quali sono le minacce? (Es.: Trascrizione errate)
Esattezza →	Corruzione dei dati: quali sono le minacce alla correttezza dei dati?
Disponibilità →	Disponibilità: quali sono i pericoli che mettono a rischio al disponibilità? Quali sono i tempi di accesso al backup?
Conformità →	Conformità: il dato risponde a regolamentazioni, anche locali?

Adattato da ISO/IEC 25012

Altre definizioni

- **Profilazione** : qualsiasi forma di trattamento automatizzato di dati personali [...] per valutare [....] il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti [...]
- **Titolare**: [...] determina le finalità e i mezzi del trattamento di dati personali (es.: l'azienda che fa le operazioni)
- **Responsabile**:[...] tratta dati personali per conto del titolare del trattamento
- **Terzo**: [...] persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (es.: un collaboratore)

Cosa è un DATA BREACH

- **Data Breach:** violazione di sicurezza che comporta accidentalmente o in modo illecito la **distruzione, la perdita, la modifica, la rivelazione** non autorizzata o **l'accesso** ai dati personali […]

[adattato da ISO27040]

REPUTAZIONE

Scenario

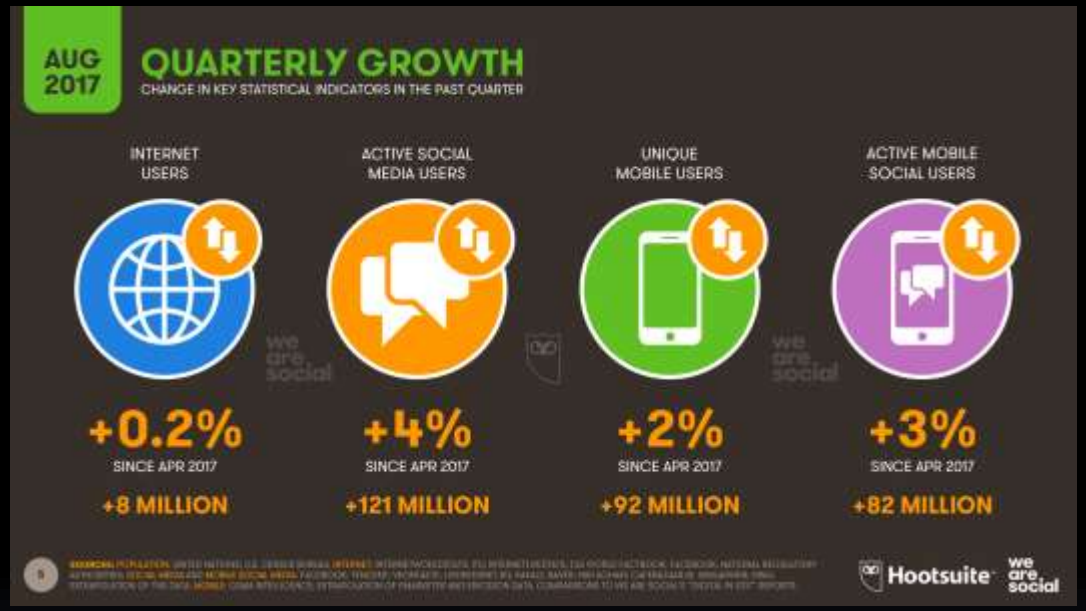
Superati globalmente

4 mld

Di utenti internet

(fonte We Are Social 2018)

Cresce la cultura social

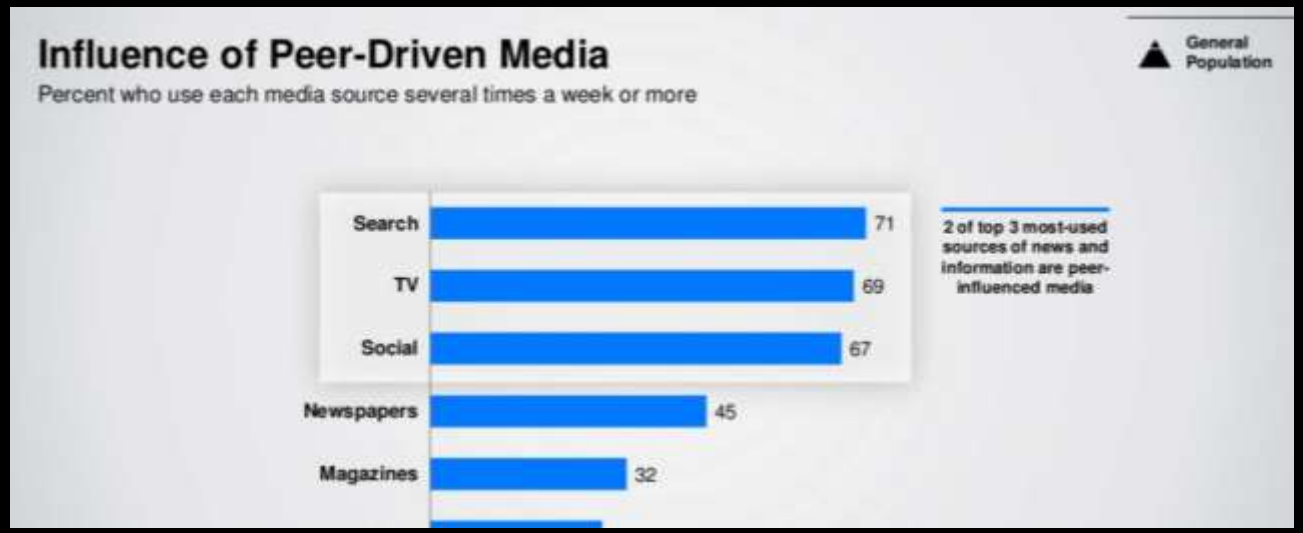


04/2017 vs. 08/2017

- 11 nuovi utenti ogni secondo
- Internet active users: **+8 mln**
- Active Social media users: **+4,0%**
- Utente solo mobile: +2%
- Active mob. Social users: **+3%**

(fonte We Are Social 2018)

Le fonti di informazione



GOOGLE è più affidabile della stampa tradizionale

La fonte di informazione principale, alla quale il pubblico si rivolge più volte a settimana sono i motori di ricerca (71%), seguiti da televisione (69%) e social network (67%)

Perché l’accento cade sui diritti e libertà

- Diritti degli interessati sono: accesso, cancellazione-oblio, limitazione del trattamento, opposizione, portabilità
- La diffusione di dati su piattaforme digitali, che hanno una persistenza potenzialmente infinita ed una diffusione mondiale, può portare a gravi conseguenze
- L’analisi del comportamento di navigazione porta ad accumulare anche dati che l’interessato non immagina

Agenda

- Privacy: cosa è cambiato in 14 anni
- Dati, Reputazione diritti e libertà personali
- Concetto di Accountability (responsabilità) e proattività
- Nuovo approccio metodologico e concetto di rischio
- Nuova figura del DPO e Registro del trattamento
- Azioni concrete (formare, documentare, controllare)

Responsabilità

- La responsabilità del titolare è una delle novità del GDPR
- Richiede conoscenza approfondita delle persone, dei processi, della tecnologia
- Richiede collaborazione trasversale
- Responsabilità di tutti i soggetti coinvolti nei processi aziendali
- Impatto su ogni aspetto aziendale e di compliance
- Definizione di processi aziendali che supportino gli obblighi di compliance
- Tecnologia per la collaborazione trasversale e crowdsourcing

Proposizione

- Il titolare del trattamento adotta metodologie e attua misure adeguate per garantire ed **essere in grado di dimostrare** che il trattamento dei dati personali effettuato è conforme allo stesso Regolamento
- La "trasparenza" intesa come garanzia della completa accessibilità alle informazioni, in primo luogo per i cittadini
- La "responsività" intesa come la capacità **di rendere conto di scelte**, comportamenti e azioni e di risponderne ad ogni figura coinvolta nel business
- La "compliance" intesa come capacità di far rispettare le norme: sia nel senso di agire per l'obiettivo stabilito nelle leggi, che nel senso di fare osservare le regole di comportamento degli operatori
- Elaborazione di specifici modelli organizzativi (analogia con d. lgs. 231/2001)

Agenda

- Privacy: cosa è cambiato in 14 anni
- Dati, Reputazione diritti e libertà personali
- Concetto di Accountability (responsabilità) e proattività
- Nuovo approccio metodologico e concetto di rischio
- Nuova figura del DPO e Registro del trattamento
- Azioni concrete (formare, documentare, controllare)

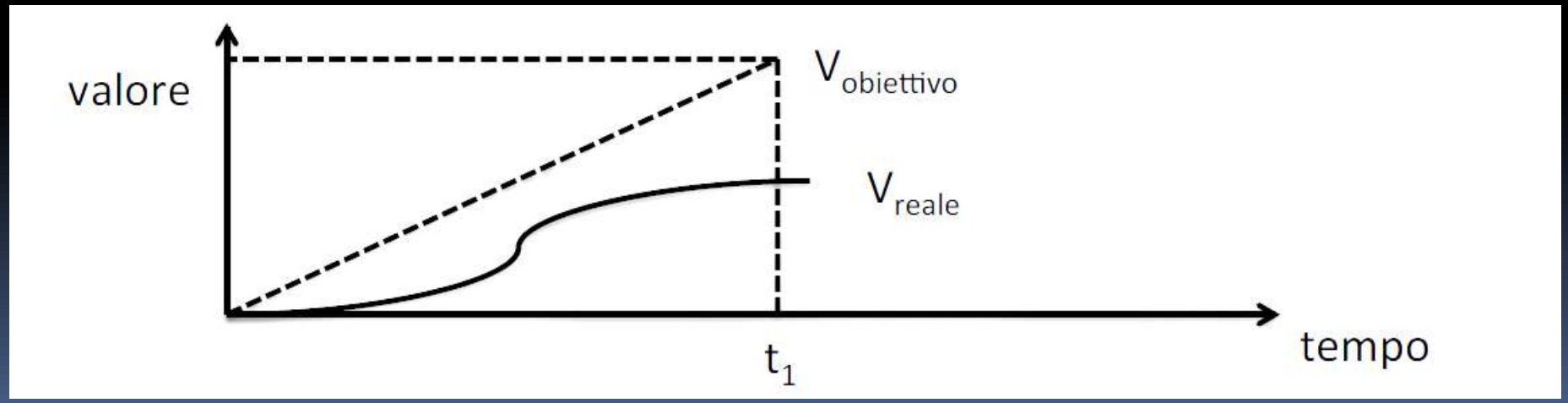
Autovalutazione

- Responsabilità del titolare e del responsabile
- Conoscenza dei flussi dati: dei trattamenti applicati
- Analisi del rischio (rif. ISO 27001:2014 e ISO31000:2009)
- Misure «appropriate» rispetto alle situazioni
- Al mutare dei trattamenti la sicurezza si deve adeguare

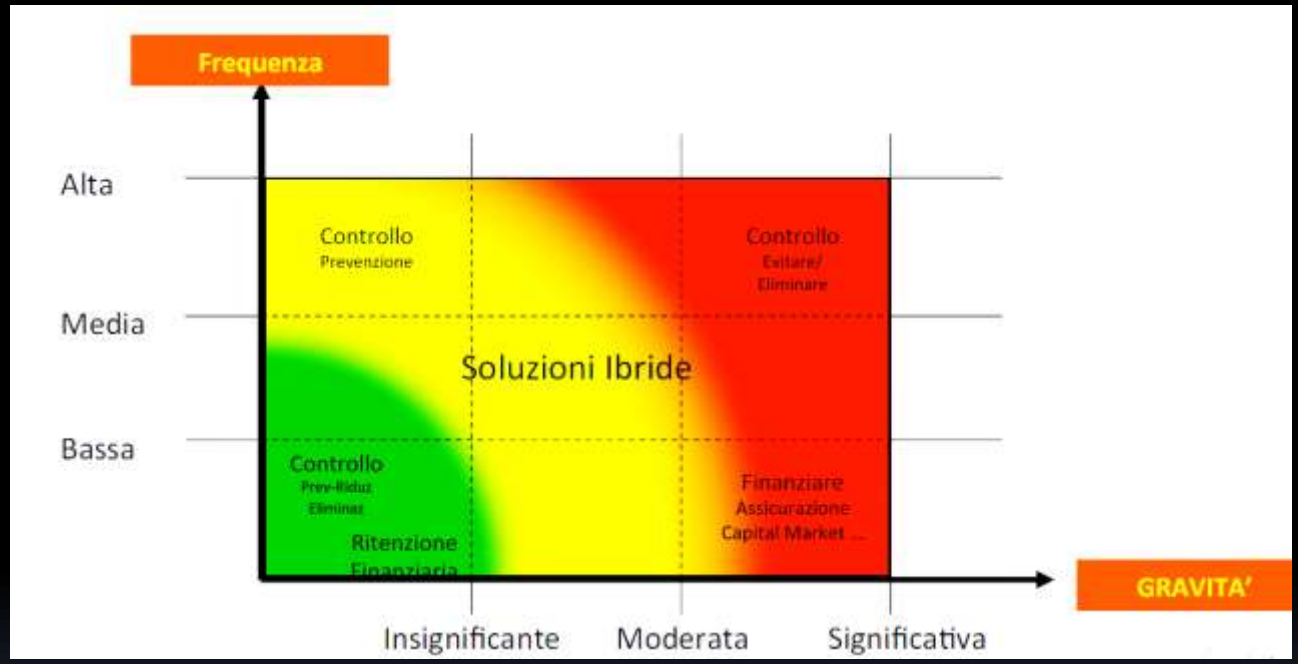
Il concetto di rischio

- Il rischio è l'**effetto dell'incertezza sugli obiettivi** (ISO 31000:2009 e ISO 27001:2014): **scostamento** da quanto atteso - positivo e/o o negativo

$$R = f * M$$

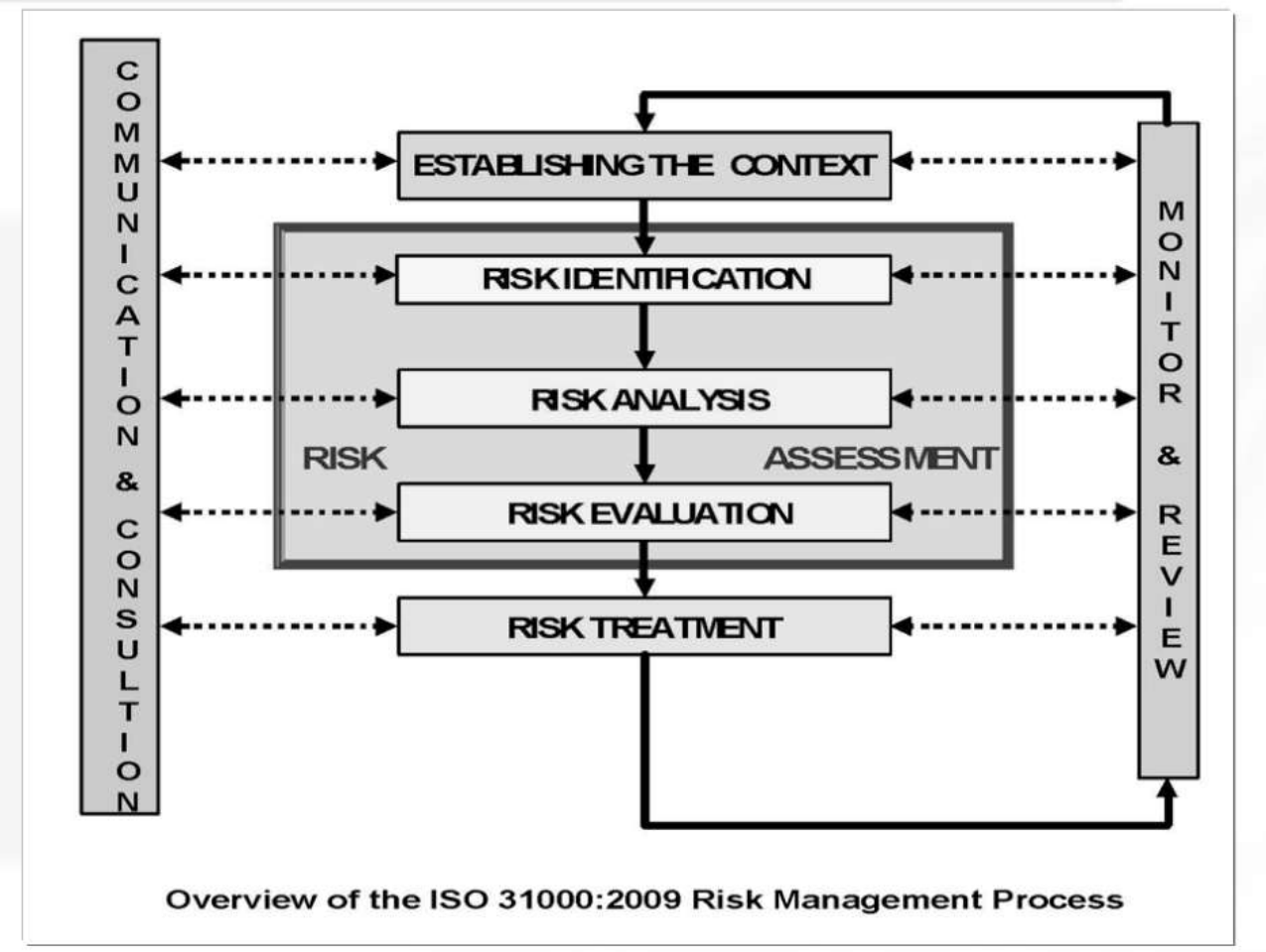


Soglia di rischio accettabile



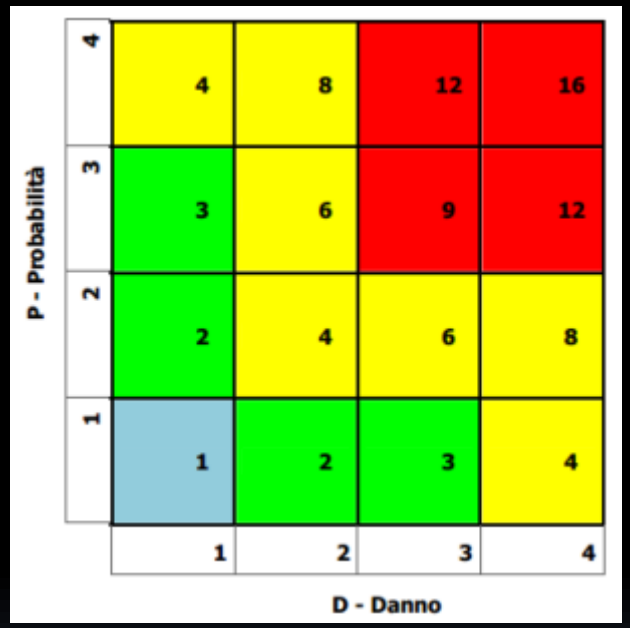
Risk Appetite = soglia di rischio accettabile sotto la quale assumo il rischio steso

Processo di analisi del rischio



Overview of the ISO 31000:2009 Risk Management Process

Analisi rischi e azioni di mitigazione



Remediation

Minaccia	Controllo di sicurezza	Rischio attuale	Rischio atteso	Azione	Da Fare Entro	Responsabile Azione
Perdita di dati per Malfunzionamento del software di archiviazione	nessuno	2*3 = 6	1*3=3	Modifica del software: Lo studio di fattibilità è stato completato e il piano per lo sviluppo è stato emesso	Gennaio	Responsabile IT

Agenda

- Privacy: cosa è cambiato in 14 anni
- Dati, Reputazione diritti e libertà personali
- Concetto di Accountability (responsabilità) e proattività
- Nuovo approccio metodologico e concetto di rischio
- Nuova figura del DPO e Registro del trattamento
- Azioni concrete (formare, documentare, controllare)

DPO

- Il DPO garantire compliance, è il riferimento interno per ogni questione o dubbio riguardante la protezione dati ma anche autorità di controllo
- Il DPO lo sceglie il titolare del trattamento
- E' obbligatorio quando
  - il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
  - le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;
  - le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Registro dei trattamenti

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità

- Bbbligo per organizzazione sopra i 250 dipendenti o dove il trattamento presenti rischi per i diritti e libertà dell'interessato
- Il nome e i dati di contatto del titolare del trattamento;
- Le finalità del trattamento;
- Una descrizione delle categorie di interessati e delle categorie di dati personali;
- Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- I trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- I termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative adeguate

Agenda

- Privacy: cosa è cambiato in 14 anni
- Dati, Reputazione diritti e libertà personali
- Concetto di Accountability (responsabilità) e proattività
- Nuovo approccio metodologico e concetto di rischio
- Nuova figura del DPO e Registro del trattamento
- Azioni concrete (formare, documentare, controllare)

Maggiore consapevolezza

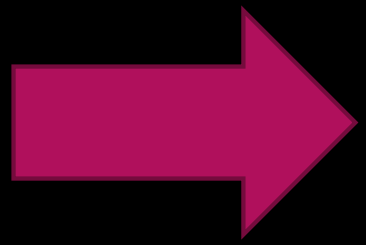
- Definire in modo chiaro la struttura organizzativa
- Identificare i processi che implicano il trattamento dei dati personali
- Definire gli attori coinvolti nei processi e le loro responsabilità
- Definire le azioni di controllo e le sanzioni

	Informazioni	Principi e politiche	Processi e procedure	Ruoli e strutture organizzative	Servizi, applicazioni e infrastrutture	Persone, abilità e competenze
Identificare						
Proteggere						
Monitorare e rilevare						
Reagire e rispondere						
Ripristinare						

Definire l’obiettivo

Situazione attuale

- Adozione dalla 196 (tra cui il DPS)
- Videosorveglianza
- Consapevolezza dei processi
- Certificazioni ISO esistenti
- Formazione (231, 626 o 196)



Obiettivo

- Manutenere la 196
- Definire l’obiettivo
- Formare tutti gli attori coinvolti nel «processing»
- Valutazione rischi
- Definire le azioni di controllo

Piano attività di adeguamento

Partendo dallo stato attuale e avendo chiaro l'obiettivo si può definire dei passi che portano all'adeguamento, prefiggendosi dei tempi

		Mesi								
Fase	Attività	1	2	3	4	5	6	7	8	9
1. Fase conoscitiva	Individuazione dei processi									
	Mission e Politica per la qualità									
	Organigramma									
2. Predisposizione della documentazione tecnica	Messa a punto metodologie di analisi									
	Attività di consulenza									
	Attività di formazione									
3. Predisposizione della documentazione di sistema	Gestione di documenti, registrazioni, dati									
	Sviluppo e mantenimento delle competenze									
	Non conformità e azioni di miglioramento									
	Processo di audit									
	Riesame e piano di miglioramento									
	Manuale qualità									
4. Implementazione delle procedure stabilite	Procedure tecniche									
	Procedure di sistema									
5. Audit interno	Programmazione dell'audit interno									
	Conduzione dell'audit interno									
	Gestione delle risultanze dell'audit interno									
6. Riesame del sistema qualità	Preparazione del riesame del sistema qualità									
	Conduzione del riesame del sistema qualità									
7. Processo di certificazione	Contatti con Organismo di Certificazione									
	Audit esterno									

Documentare i trattamenti

Funzione di business/Unità Organizzativa/Dipartimento	Denominazione del trattamento (se individuata)	Finalità del trattamento	Software, Database, Manutenzione	Denominazione e dati di contatto del contitolare (se presente)	Categorie di interessati	Categorie di dati personali	Categorie di destinatari a cui i dati sono o possono essere comunicati	Denominazione responsabili esterni (se presenti)	Paesi Terzi o organizzazioni internazionali verso cui i dati possono essere trasferiti	Indicazione garanzie adottate per il trasferimento internazionale (se applicabile)	Periodo di conservazione dei dati (se possibile)	Descrizione generale delle misure di sicurezza adottate (se possibile)
Risorse Umane, Amministrazione	Pagamento stipendi	Amministrazione del personale	Software XXX in cloud e cartelle su NAS. Manutenzione da remoto	N/A	Dipendenti	Dati relativi alla prestazione lavorativa	Previdenza sociale	Dott. XXXX (Consulente lavoro)	N/A	N/A	10 anni	1.a, 1.b, 1.c, 1.d. 1.h, 2.a, 2.b, 2.e, 2.f, 2g

Articolo 6 (base giuridica su cui si fonda il trattamento)	Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)	Tipologia di trattamento	Fonte dei dati personali (se applicabile)	Consenso degli Interessati	Modalità di conservazione dei dati	Valutazione richiesta?	Fase della Valutazione	Indicazione della Valutazione (DPIA) -estremi
Obbligo legale	Esercizio obblighi in materia di diritto del lavoro	normale -> nessuno dei tipi seguenti	N/A	N/A	Analogico e digitale	NO	N/A	

Verifiche

Prevedere verifiche su:

- La corretta applicazione dei processi
- La validità dei processi documentati (l'azienda cambia)
- La formazione delle figure coinvolte
- Ecc. ecc.

Saper giustificare le proprie scelte

Raccogliere assieme il lavoro fatto di documentazione, pianificazione, tracciatura e verifica

Il tutto serve a poter mostrare ad una verifica quanto si sta facendo e a portare prove per mostrare la propria capacità di gestione dei rischi da trattamento dei dati per garantire diritti e liberta degli individui

CONTATTI

enrico.magalini@avelia.it