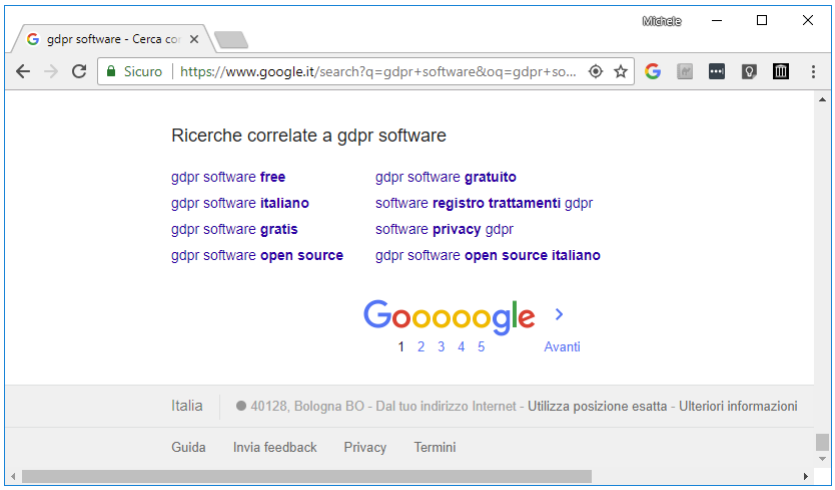
PRIVACY E STUDI LEGALI: COSA E COME FARE PER ADEGUARSI AL REGOLAMENTO EU 679/2016 (GDPR)

Le misure di sicurezza e il registro dei trattamenti dell'avvocato

Michele Ferrazzano

Bologna, 30 Maggio 2018

Scorciatoie al GDPR



Scorciatoie al GDPR

Servizio per la redazione del Registro Dei Trattamenti in conformità all'articolo 30 GDPR Privacy Europea	Una soluzione che guida la gestione della privacy in applicazione del GDPR 25 Maggio 2018	E' il servizio veloce che aiuta le piccole aziende a mettersi in regola con la normativa GDPR	Auto-valuta, ottieni e mantieni la conformità GDPR in modo semplice con aiuto legale specializzato
A partire da **€ 20,00** /mese	A partire da **€ 24,00** /mese + UT € 240,00	**€ 10,00** /mese + UT € 150,00	A partire da **€ 49,00** /mese + UT € 100,00

Prezzi IVA esclusa

QUANTI DUBBI HAI ANCORA DELLA NUOVA NORMATIVA PRIVACY

CHE ENTRERA' IN VIGORE IL 25 MAGGIO?

SEI PREOCCUPATO?! BASTANO 2 CLICK!

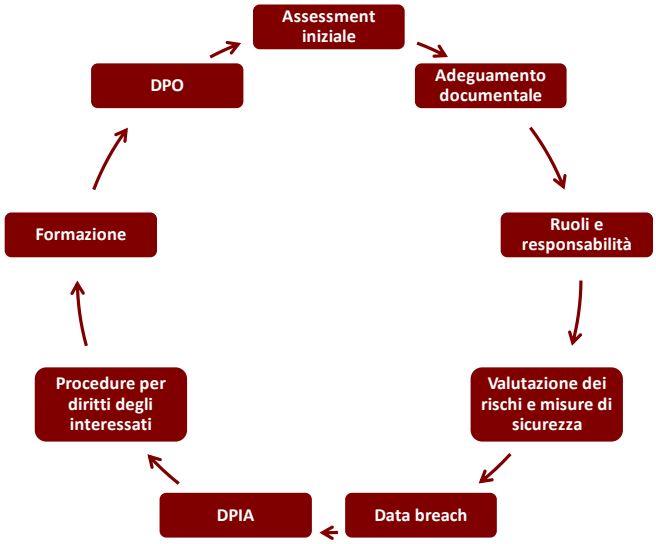
- Scarica il software
- Attiva il **modulo Privacy** comprensivo di: *creazione informativa privacy, moduli per il consenso, creazione e gestione del registro di trattamento dei dati*
- .....**FINITO!**

Il costo del servizio per tutti gli Avvocati dell'
è di 19,90 € + iva**

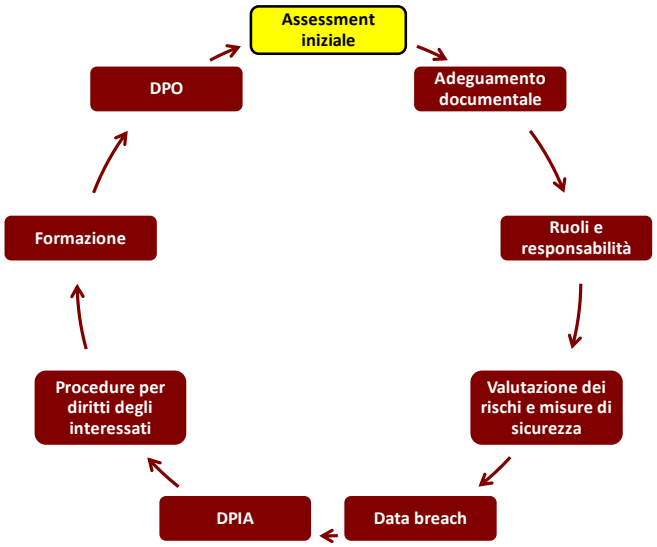
CONTATTACI

Adeguamento GDPR: la soluzione ideale

Piano di adeguamento al GDPR

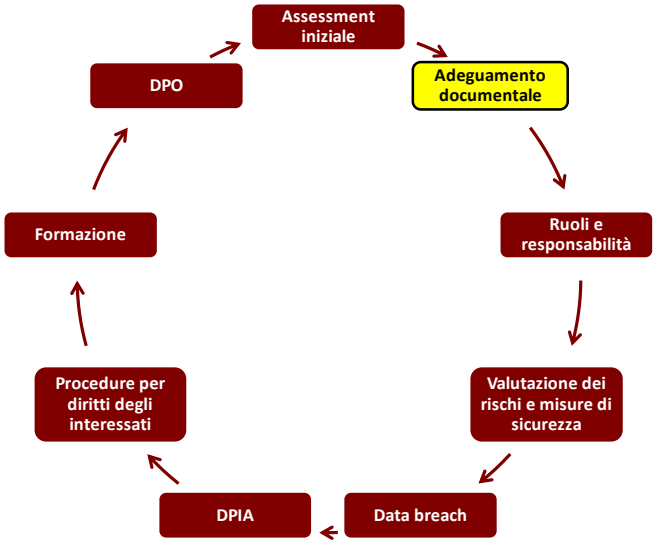


Piano di adeguamento al GDPR



Questionari e interviste per
- esaminare lo stato attuale
- conoscere in dettaglio l'attività e le procedure
- prima quantificazione del carico di lavoro per giungere all'adeguamento

Piano di adeguamento al GDPR



Registro dei trattamenti

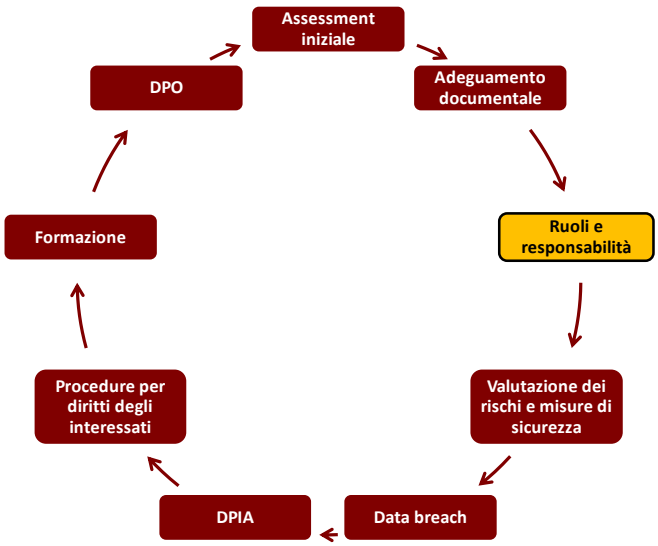
Informative

Consensi

Policy aziendali

BCR

Piano di adeguamento al GDPR

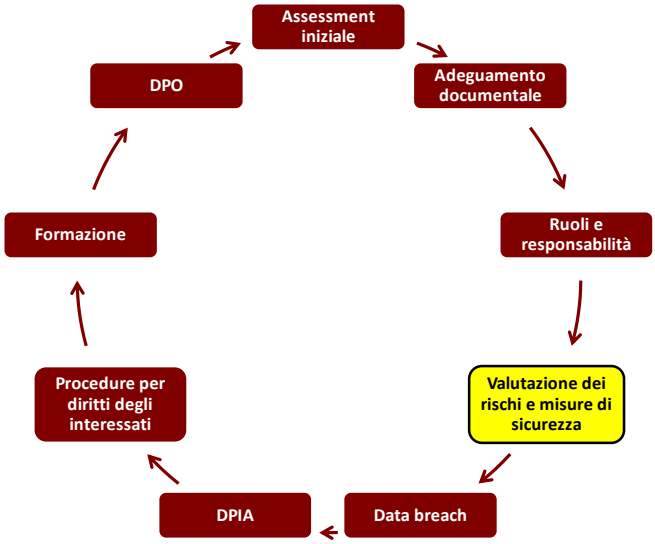


Individuare responsabili dei vari trattamenti definiti

Individuare responsabili per enti molto grandi (es. un referente per ogni stabilimento)

Individuare la figura preposta per il ruolo di DPO

Piano di adeguamento al GDPR

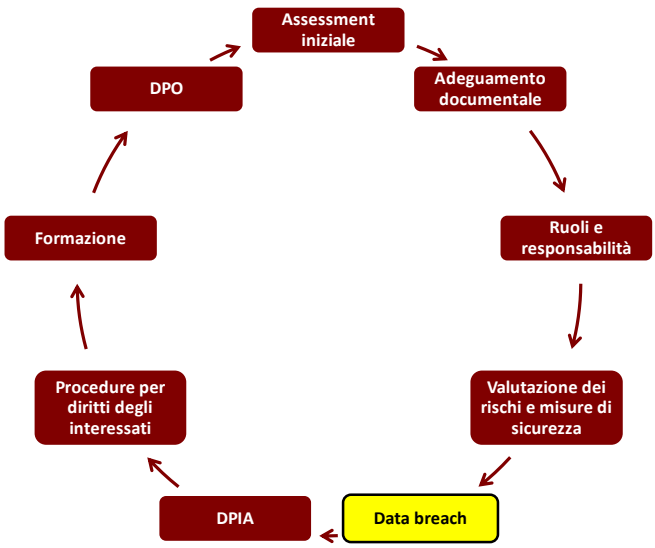


Esame dell'infrastruttura informatica e degli strumenti in uso

Identificazione delle misure tecniche/organizzative per ridurre il rischio

Implementazione di meccanismi di logging

Piano di adeguamento al GDPR

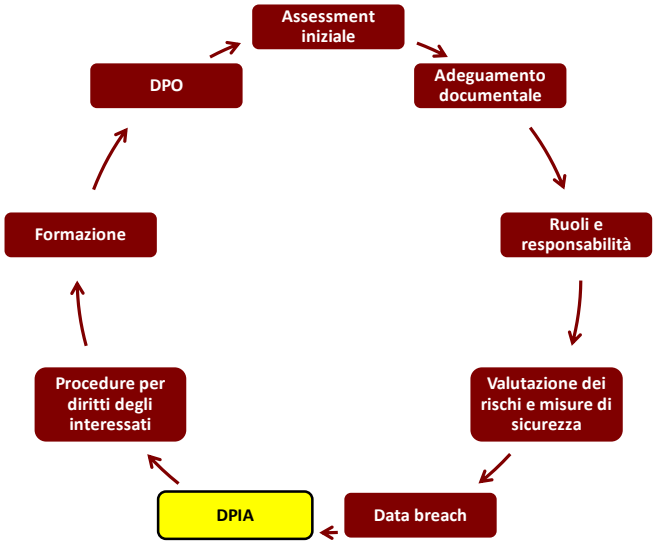


Identificazione di tutti i possibili data breach

Definizione moduli e procedure per tempestiva comunicazione ad autorità e interessato

Procedura per quantificazione del rischio e delle libertà dell'interessato

Piano di adeguamento al GDPR



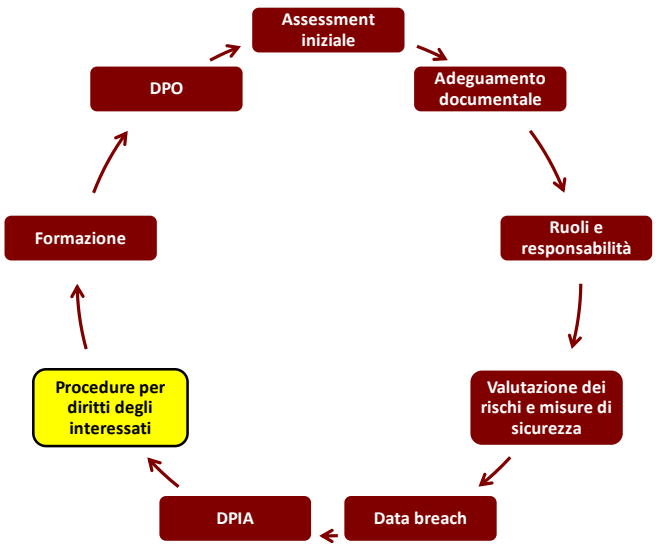
Valutazione di impatto quando si trattano particolari categorie di dati o grandi quantità di dati

Valutare se si ha obbligo di DPIA

Valutare confidenzialità, integrità e disponibilità

All'esito, potrebbe emergere esigenza di introdurre misure per mitigare il rischio o in alternativa chiedere autorizzazione preventiva al Garante

Piano di adeguamento al GDPR

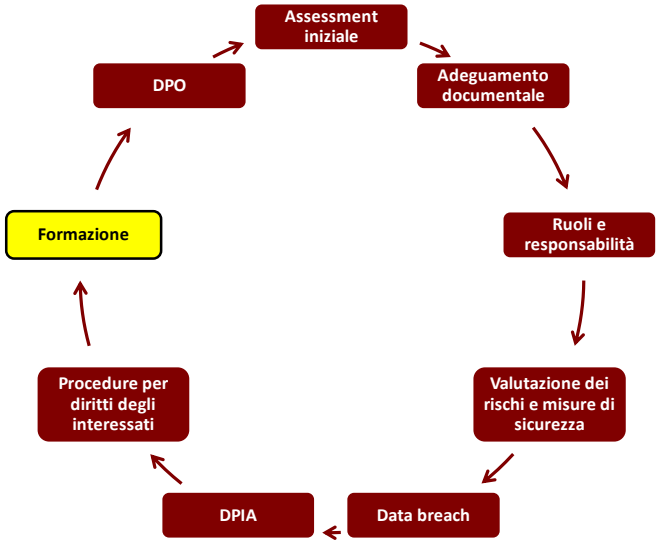


Prevedere strumenti che consentano di soddisfare rapidamente le richieste degli interessati
(es. cancellazione, rettifica, conoscenza dei dati trattati…)

Prevedere procedure e modulistica per rispondere alle esigenze degli interessati

Disporre di figure preposte a tali attività (eventualmente il DPO)

Piano di adeguamento al GDPR



Dopo aver predisposto tutto, sensibilizzare il personale e formare per rispettare le policy e conoscere le procedure da adottare

Rientra negli oneri del titolare documentare di aver effettuato idonea formazione (principio dell'**accountability**)

Piano di adeguamento al GDPR

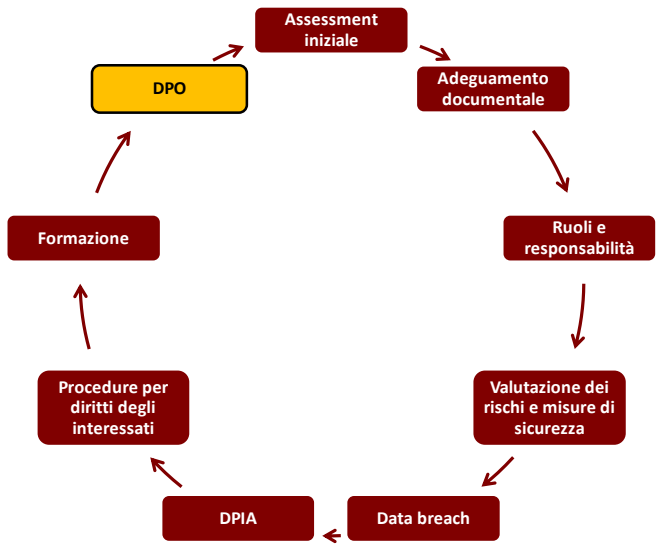


Figura non sempre obbligatoria, ma potrebbe essere comunque utile

Interfaccia con il Garante e consigliere/valutatore del Titolare

Fase 1 – Assessment iniziale

Fase 1 – Assessment iniziale

- Questionario preliminare
- Esame documentazione esistente e policy
- Colloquio con personale
  - Verificare maturità e rispetto delle policy già in essere (se ci sono)
- Esame infrastruttura informatica
  - Quali/quanti sistemi
  - Misure tecniche in essere
  - Quali trattamenti
  - Quali dati
  - …

Fase 1 – Assessment iniziale

- **Questionario preliminare**
  - *Alcuni esempi di domande:*
    - L'azienda ha più di **250 dipendenti**?
    - L'azienda opera nel **settore pubblico**?
    - Sono effettuati trattamenti che possono presentare un **rischio per i diritti e le libertà degli interessati**?
    - I trattamenti richiedono il **monitoraggio regolare, continuativo e sistematico**? (es: videosorveglianza)
    - Conosci e hai l'**elenco degli asset informatici** (sito web, server, database, postazioni lavoro, CRM,…) che concorrono nella raccolta, trasferimento, gestione, memorizzazione e trattamento dei dati?
    - È possibile usare **chiavette USB**?
    - Vengono usati sistemi di **cifratura**?
    - Come vi comportate per la gestione dei **documenti cartacei**? Dove sono conservati? Come li distruggete?
    - […]

Fase 2 – Adeguamento documentale

Fase 2 – Adeguamento documentale

- **Registro dei trattamenti**
- Informative
- Consensi
- Policy aziendali
- BCR

Fase 2 – Adeguamento documentale
Registro dei trattamenti

Ruolo	
Processo aziendale	Nome del Processo
	Responsabile del Processo (*Referente interno*)
Descrizione funzionale del Trattamento	ID
	Breve descrizione del Trattamento
	Finalità del Trattamento
	Base giuridica
	Tipo di Trattamento
Dati e Interessati	Categorie Funzionali dei Dati
	Categorie Particolari di Dati Personali
	Categorie di Interessati
	Categorie Vulnerabili di Interessati
	Livello di Classificazione dei Dati
	Periodo di Conservazione
	Combinazione di Dati
	Fonte originale
Responsabili del Trattamento	Nome
	Documento di Riferimento

Fase 2 – Adeguamento documentale
Registro dei trattamenti

Trasferimento Dati	Categorie Funzionali dei Dati trasferiti
	Categorie di Destinatari
	Paese terzo / Organizzazione Internazionale
	Natura del Trasferimento
	Riferimento
	Salvaguardie appropriate (per trasferimenti effettuati in mancanza di una decisione di adeguatezza)
Tecnologie utilizzate	Descrizione
Rischi e misure mitigative	Rischio
	Descrizione delle Misure mitigative
	Documentazione di Riferimento
	Risultati DPIA
Diritti degli Interessati	Informativa
	Procedure per l'Esercizio dei Diritti
Stato	Data di inizio Trattamento
	Data di fine Trattamento
	Trattamento alternativo
	Data di ultimo aggiornamento della riga

Fase 4 – Valutazione dei rischi e misure di sicurezza

Fase 4 – Valutazione dei rischi e misure di sicurezza

- Rispetto al Codice Privacy non sono più previste le c.d. **misure minime**
- Il Titolare del trattamento ha la responsabilità (*accountability*) di definire:
  - **rischi**
  - **misure adeguate**, ovvero
    - **adeguate** alla struttura del Titolare
    - elaborate **caso per caso**
    - attuate **in base a mappatura dei dati trattati, mole degli stessi e dei rischi** di trattamento dei dati gestiti
- **Accountability** significa essere in grado di "rendere conto" delle attività poste in essere e del fatto di aver rispettato i principi del GDPR

Fase 4 – Valutazione dei rischi e misure di sicurezza

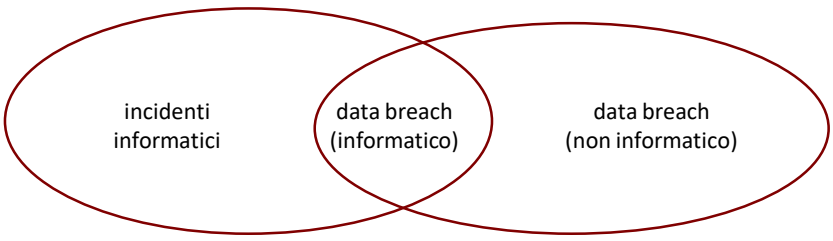
- **Misure di sicurezza**
  - Sicurezza del sistema e delle applicazioni
    - Aggiornamenti
    - No software craccato
    - Ridurre al minimo (eliminare) software «free» reperito in rete
      - Possibile vettore di malware
  - Sicurezza delle comunicazioni
    - Apparati hardware idonei (es. firewall)
    - VPN
  - Confidenzialità dei dati
    - Cifratura
  - Sicurezza dei sistemi terzi adottati
    - Valutare gestore di posta elettronica
    - Cloud storage…
  - Sicurezza nella disponibilità dei dati gestiti
    - Backup e ripristino
    - Dislocazione geografica

Fase 5 – Data breach

Fase 5 – Data breach

- **Incidente informatico**
  - Qualsiasi evento che
    - riduce la funzionalità del sistema informatico
    - rende i dati non disponibili/inaffidabili
    - rende pubblici dati riservati

- **Data breach**
  - Particolare tipo di incidente (informatico o non) che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati



Fase 5 – Data breach
Statistiche su data breach in Italia

41	UniCredit SpA	400,000	07/09/17	Identity Theft	Malicious Outsider	Italy	Financial	7.8
314	Wind Tre	5,118	03/20/17	Account Access	Malicious Outsider	Italy	Technology	5.6
1554	Corregio Police Department	Unknown	12/30/17	Identity Theft	Malicious Outsider	Italy	Government	1.9
1610	Italian Prime Minister's Office	Unknown	11/17/17	Identity Theft	Accidental Loss	Italy	Government	1.6

Fase 5 – Data breach
Tipi di data breach

- **Confidentiality Breach**
  - accesso accidentale o abusivo a dati personali
- **Availability Breach**
  - perdita o distruzione accidentale o non autorizzata del dato personale
- **Integrity Breach**
  - alterazione accidentale o non autorizzata del dato personale

Fase 5 – Data breach
Esempi di data breach

	Confidentiality breach	Availability breach	Integrity breach
Invio email a indirizzo non corretto	x		
Perdita di una chiavetta USB	x	x	
Sovrascrittura file per errore		x	x
Collaboratore cancella archivio		x	x
Collaboratore copia dati prima di andar via dallo studio	x		
Computer infettato da malware	x	x	x
Dimentico il fascicolo cartaceo in tribunale	x	x	
Incendio in studio (senza avere backup)		x	
Furto in studio	x	x	
Furto del PC (cifrato)		x	
Furto del PC (cifrato), ma ho i backup			

Fase 5 – Data breach
Prevenire data breach

- **Confidentiality Breach**
  - accesso accidentale o abusivo a dati personali
- **Availability Breach**
  - perdita o distruzione accidentale o non autorizzata del dato personale
- **Integrity Breach**
  - alterazione accidentale o non autorizzata del dato personale
- **Prevenzione** significa:
  - Evitare accesso accidentale o abusivo
  - Evitare perdita o distruzione
  - Evitare alterazione

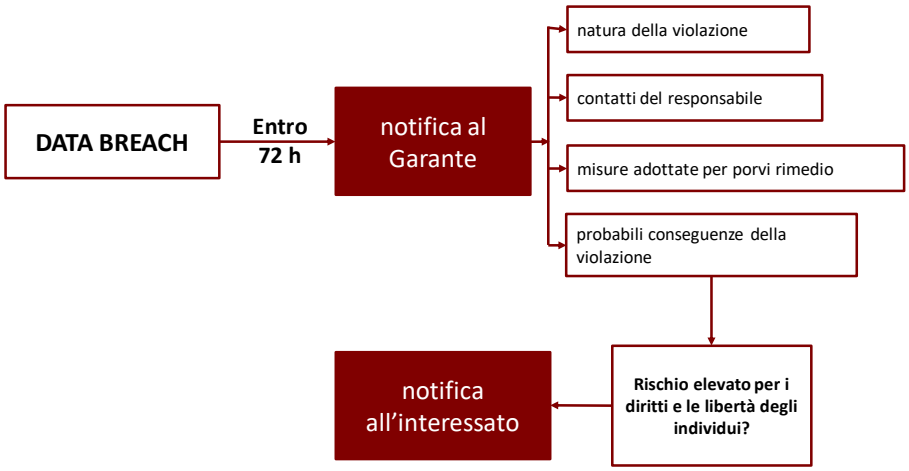
Fase 5 – Data breach
Prevenire data breach

** I prodotti/vendor elencati sono a scopo esemplificativo e rappresentano un sottoinsieme di quelli disponibili sul mercato e potrebbero non essere adatti alle vostre necessità*

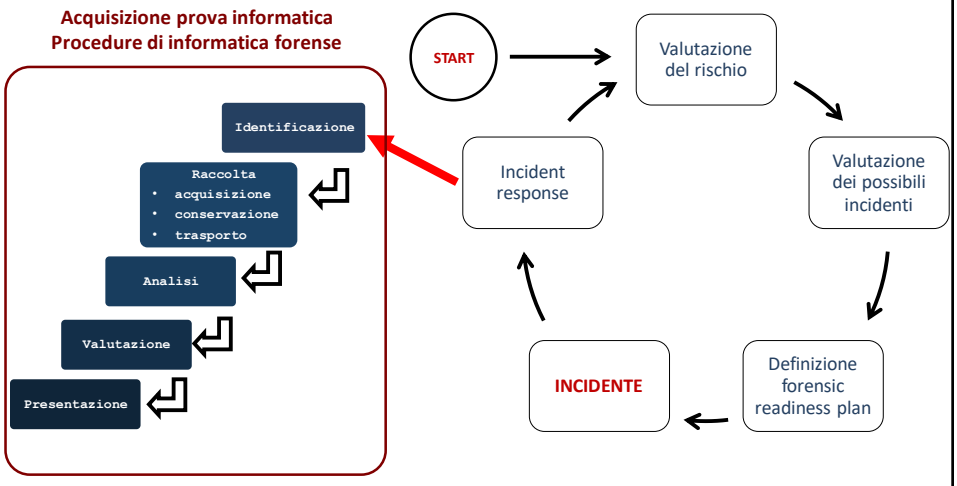
Problema	Soluzione tecnica	Prodotti*
Perdita/furto notebook	Cifratura del disco	Bitlocker, Dell Data Protection, Sophos SafeGuard
Perdita/furto smartphone	Mobile Device Management e cifratura	Airwatch, Mobile Iron, Google Suite
Virus / Ransomware	Antivirus centralizzato con funzionalita anti ransomware	Sentinel One, Kaspersky, Symantec, Sophos
Sovrascrittura accidentale	Sistemi di versioning	Google Suite
Cancellazione file	Sistemi di versioning / Backup	Google Suite, OneDrive,
Cancellazione messaggio di posta elettronica	Vault	Google suite, Office 365
Perdita disponibilità dato	Data Loss Prevention Data governance	Symantec, McAfee, Varonis, Nuix
Accessi abusivi a rete aziendale	Firewall	Sonicwall, Cisco, Palo Alto
Controllo accessi	SIEM / Log management	Splunk, Logrythm, Logstash
Controllo accessi	2FA	Vasco, Yubi, RSA

Fase 5 – Data breach
Obblighi in caso di data breach

Notifica al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui si ha notizia



Fase 5 – Data breach
Obblighi in caso di data breach



Fase 6 – DPIA
(Data Protection Impact Assessment)

Fase 6 – DPIA
Che cosa è un DPIA?

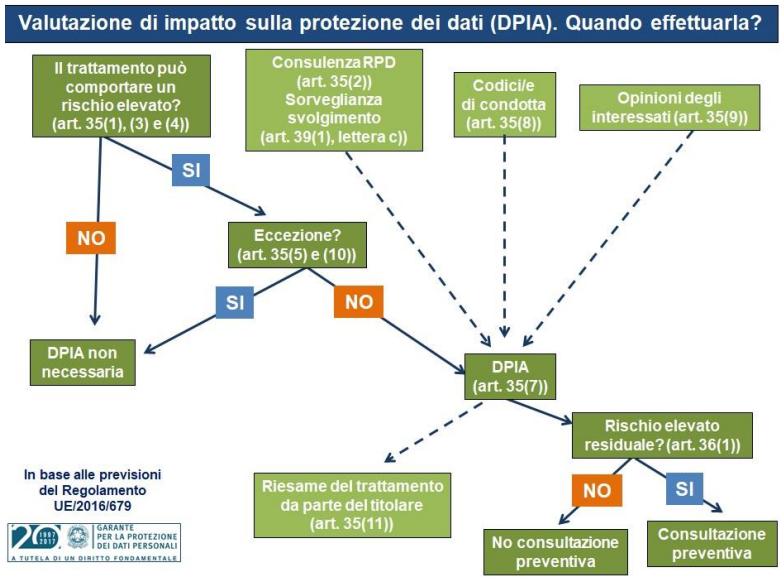
- **Processo** per:
  - descrivere un trattamento
  - valutare la necessità e proporzionalità di un trattamento
  - aiutare nella gestione dei rischi ai diritti e alla liberta delle persone conseguenti al trattamento di dati personali
  - valutare i rischi e determinare le misure per indirizzarli
- Strumento per dimostrare l'**accountability** ai requisiti del GDPR
- Processo per costruire e dimostrare **compliance**

Fase 6 – DPIA
Quando fare una DPIA

- Una DPIA deve essere
  - **completata prima dell'inzio di un trattamento** che possa comportare un alto rischio ai diritti e alle libertà delle persone fisiche
  - **eseguita quando riguarda l'adozione di nuove tecnologie**
  - **aggiornata regolarmente** in presenza di **variazione** alle sopra indicate circostanze
- Una DPIA può comprendere un insieme di trattamenti che presentino rischi simili

- **Necessaria quando**
  - una **valutazione sistematica e globale di aspetti personali** relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche
  - il **trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati**
  - la **sorveglianza sistematica** su larga scala di una zona accessibile al pubblico

Fase 6 – DPIA



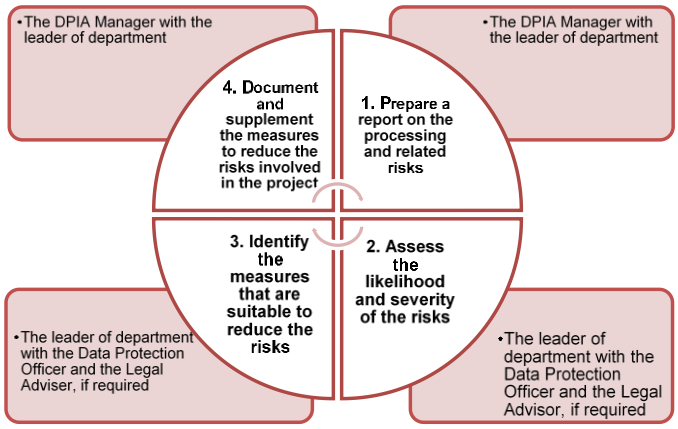
Fase 6 – DPIA
Quando fare una DPIA

- Qualunque trattamento a rischio elevato
- Ognuno deve fare le proprie valutazioni di opportunità
- Consigliato effettuare una DPIA anche quando non esplictamente richiesto dal GDPR

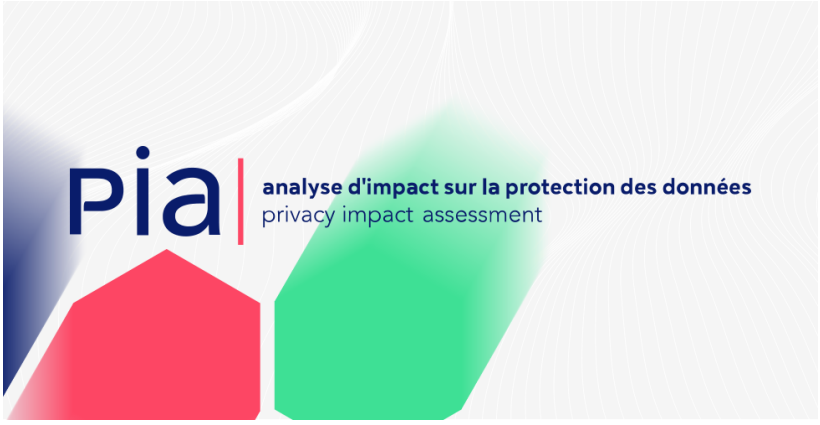
Fase 6 – DPIA
DPIA Quiz

- Caso 1
  - Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet…
- Caso 2
  - Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web

Fase 6 – DPIA
Ciclo di una DPIA

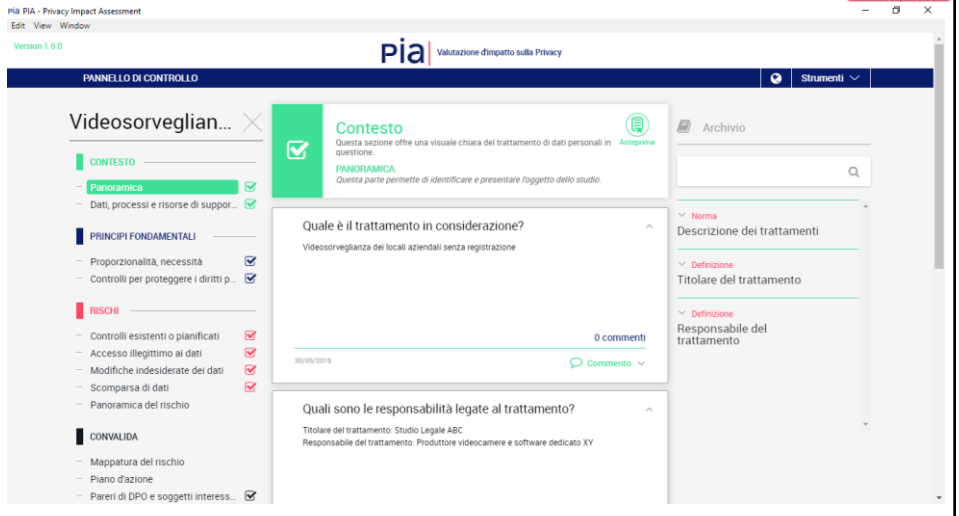


Fase 6 – DPIA
DPIA Tool

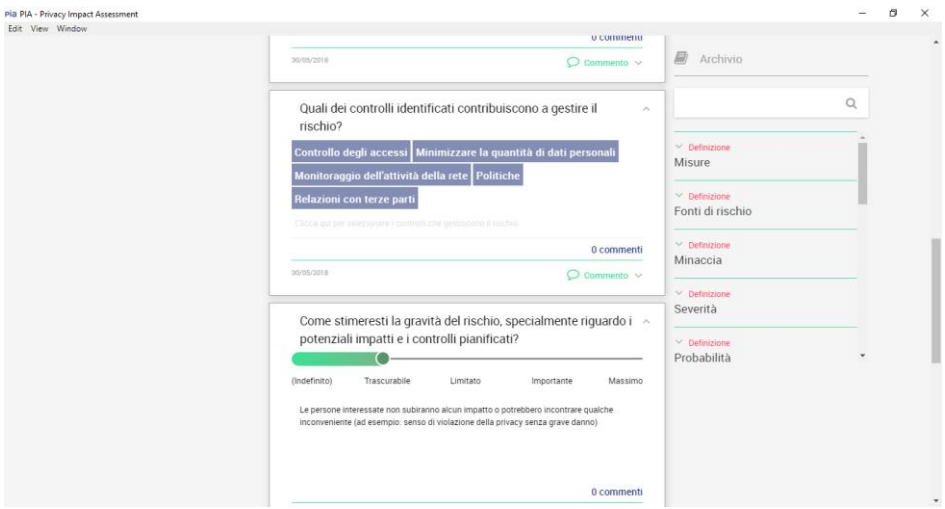


Esempio DPIA

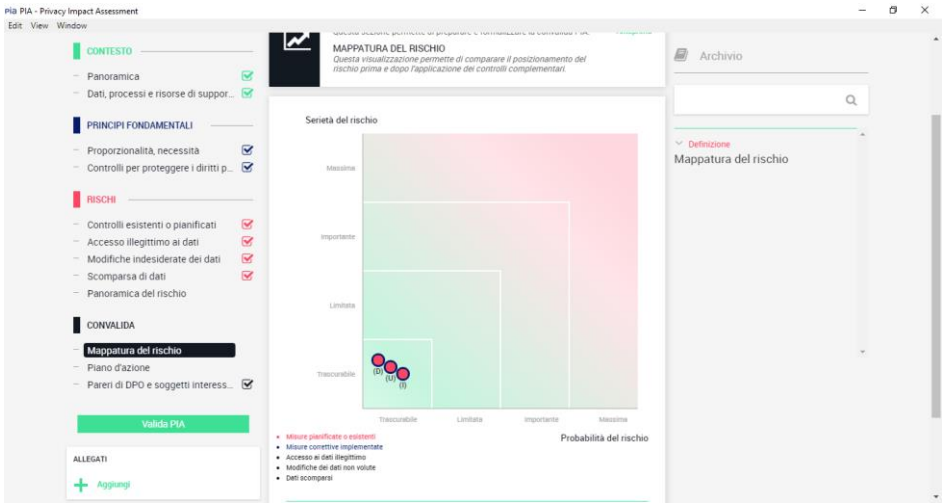
Esempio DPIA



Esempio DPIA



Esempio DPIA



Fase 7 – Procedure per diritti degli interessati

Fase 7 – Procedure per diritti degli interessati
Diritti dell'interessato

ACCESSO

sapere quali dati sono stati raccolti, come e da chi sono trattati, per quanto tempo saranno mantenuti

CONSENSO

ottenere un'informativa chiara, redatta con un linguaggio semplice e poter revocare il consenso in qualsiasi momento

RETTIFICA

correggere i dati personali inesatti

CANCELLAZIONE

chiedere la cancellazione dei dati personali nei casi previsti

PORTABILITÀ

ricevere i dati personali in un formato leggibile da un dispositivo automatico per trasmetterli ad altro titolare del trattamento

PROCESSO AUTOMATIZZATO

non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato

Fase 7 – Procedure per diritti degli interessati

- Definire processo per rispondere rapidamente e dettagliatamente alle richieste pervenute
  - Avvalersi del registro dei trattamenti per verificare processi e luoghi in cui è presente dato dell'interessato

Fase 8 – Formazione

Fase 8 – Formazione

- Illustrare aspetti cruciali GDPR
- Illustrare policy e regolamenti
- Verificare (anche a campione e/o a sorpresa) rispetto di policy e regolamenti


CONOSCO UN ESPERTO DI GDPR
MI PUOI DARE LA SUA EMAIL?


CONOSCO UN ESPERTO DI GDPR
MI PUOI DARE LA SUA EMAIL?
NO.

Riferimenti utili

- «Il GDPR e l'avvocato»; http://www.consiglionazionaleforense.it/web/cnf/-/gdpr-avvocati-proget-1
- «Linee guida per la Data Protection Impact Assessment»; (Osservatori.net, Polimi)
- «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679»; http://194.242.234.211/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati
- **«Regolamento UE. Un software per la valutazione di impatto»** http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8581268

BIT4LAW S.r.l.
Via Giuseppe Brini, 45
40128 – Bologna – BO
http://www.bit4law.com
☏ +39 051 0562070 – 🖷 +39 051 0822768
info@bit4law.com – bit4law@pec.it
P.I.: 03434841205 – REA BO 518648