EcoSafe®

Abbiamo il pallino di un futuro migliore

Processi, Tool, Servizi Professionali

GDPR Compliance: Cosa significa?

- Applicazione dei principi del GDPR:
  - accountability (GDPR, art. 24)
  - Data protection by design (GDPR, art. 24 par. 1)
  - Data protection by default (GDPR, art. 24, par. 2)

- Obiettivi:
  - Adeguamento tecnico-processivo del sistema di gestione della data protection aziendale
  - Acquisizione della capacità di dimostrare la compliance
  - (opzionale) Certificazione (cfr. GDPR art. 24 par. 3)

GDPR Compliance: un processo modulare

- General Assessment: analisi per formulazione offerta e pianificazione
- Gap Analysis: verifica del divario fra as-is e situazione target
- Mapping dei trattamenti: identificazione e registrazione dei trattamenti
- Risk Analysis e DPIA: analisi dei rischi per gli interessati
- Organigramma della data protection: definizione dei ruoli, job description
- Revisione documentale: informative, regolamenti, deleghe
- Data breach management: processo di gestione delle violazioni dei dati
- Piano di mantenimento e miglioramento: formazione e audit

General Assessment

- Analisi dell'operatività aziendale
  - attività core
  - attività di supporto
- Tipologie di dati trattati
  - natura dei dati trattati
  - (quantità di dati)
- Tipologia degli interessati
  - categorie vulnerabili
  - (volumi)
- Organizzazione:
  - Sedi nazionali
  - Sedi internazionali (UE/Extra-UE)
- Sistemi informativi
  - archivi documentali
  - descrizione del sistema IT
  - Asset Inventory
- Fornitori
  - Tipologia di servizi in outsourcing
- Tipologia dei Clienti
  - Servizi erogati come Titolare
  - Servizi erogati come Responsabile
- Certificazioni (ISO 9001:2015, 27001, etc.)
- Adesioni a codici di condotta (art. 40)

GDPR Compliance: GAP Analysis

GAP Analysis normativa: strumenti per la raccolta informazioni intesa a individuare la distanza che separa l'AS-IS dalla piena compliance normativa (adatta a realtà più complesse)

- Regulatory Compliance Tool

GAP Analysis tecnologica: strumenti per la raccolta informazioni intesa a individuare la distanza che separa l'AS-IS dalla piena compliance tecnologica

- Standard di riferimento: Questionario AgID per la PA

GDPR Compliance: Mapping

- mappatura dei trattamenti di dati personali
- cfr. GDPR Art. 30: Registro delle attività di trattamento
  - Registro dei Titolare
  - Registro del Responsabile
- Strumento
  - di compliance
  - di dimostrazione della compliance
- Tool: **Zeus**

Considerando 82: Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.

GDPR Compliance: Risk Analysis

- Analisi dei rischi cui sono esposti
  - gli interessati
  - l'organizzazione
- cfr. GDPR art. 32 par. 1
- Individuazione di un sistema di riferimento che tenga conto di quanto previsto dall'art. 32 par. 2
  - Esempio: 31000, 27001 (VERA)

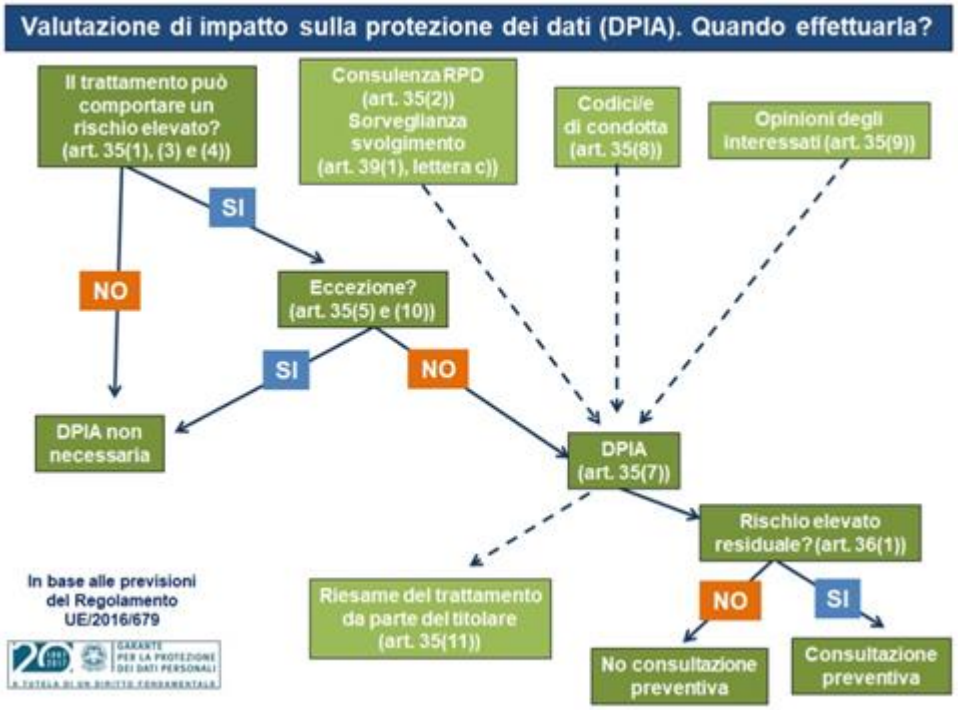
Considerando 83: Per mantenere la sicurezza [...] il titolare o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali **trasmessi**, **conservati** o **comunque elaborati** che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

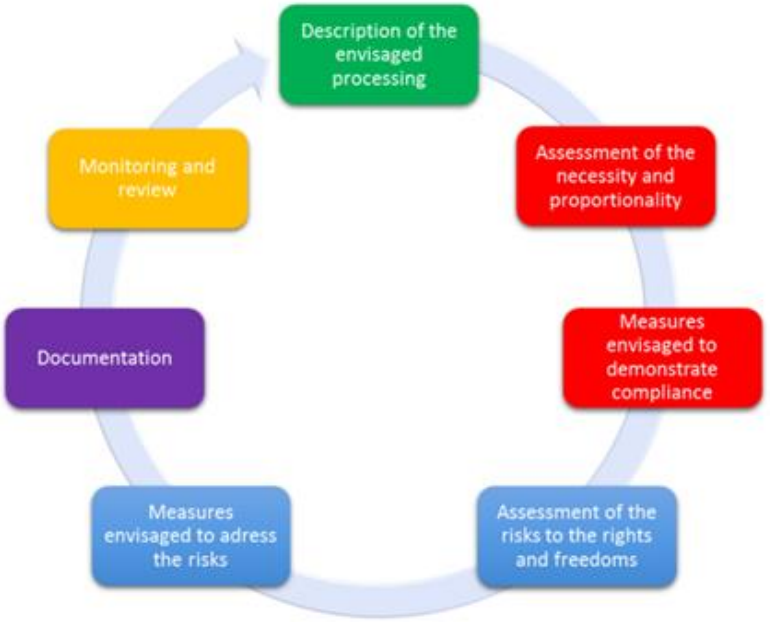
GDPR Compliance: DPIA (1)

Data Protection Impact Assessment (Valutazione d'impatto sulla protezione dei dati):

- In carico al Titolare
- cfr. GDPR art: 35, Considerando 84, 89, 93 e 95
- Obbligatoria quando il trattamento comporta un rischio elevato per le libertà e i diritti delle persone fisiche
- cfr. WP29: il "metodo del 2"
- Metodo: CNIL

GDPR Compliance: DPIA (2)





Tool: CNIL

GDPR Compliance: Organigramma della DP

Individuazione e definizione dei ruoli e delle mansioni.

In particolare:

- degli owner del trattamento, possibili delegati del Titolare
- degli owner del trattamento e delle U.O. coinvolte, da autorizzare
- dei responsabili esterni da incaricare
- del DPO da nominare (se previsto)

Tool: **Zeus**

GDPR Compliance: revisione documentale

Revisione e integrazione dell'impianto documenta esistente.

- Lettere di delega e lettere di incarico (responsabili esterni)
- Informative (cfr. GDPR art. 13 - 14)
- Lettera di nomina del DPO (se previsto)

Opzionali:

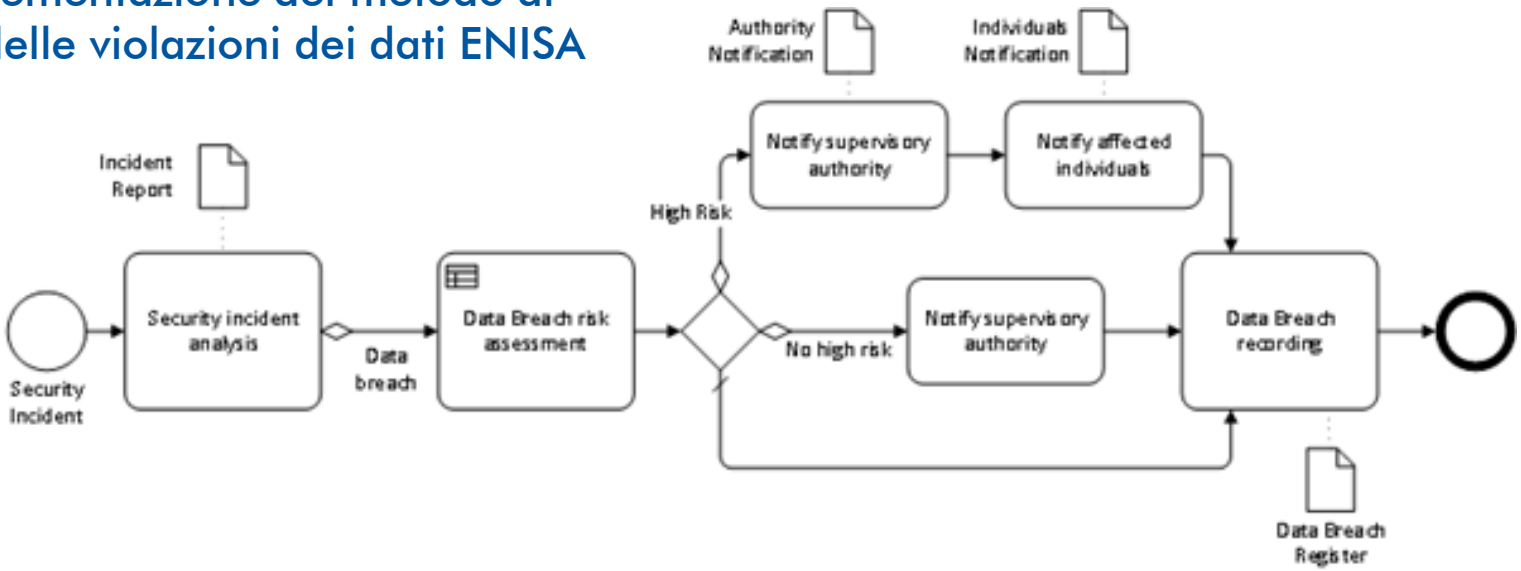
- Regolamenti interni (e.g. **manuale di comportamento**)
- Evoluzione del processi di qualificazione dei fornitori

Tool: **template**, **repository documentale (Zeus)**

GDPR: data breach e piano di verifica

- Gestione della data breach (cfr. GDPR artt. 33-34, WP29)
- Formazione del personale autorizzato
- Formazione del DPO
- Pianificazione degli audit

Tool: implementazione del metodo di gestione delle violazioni dei dati ENISA



GDPR Compliance: il DPO

Data Protection Officer:

- cfr. DPR art. 37: designazione
- cfr. DPR art. 38: Posizione
- cfr. DPR art. 39: Compiti
- DPO interno (formazione) vs DPO esterno (professional service)

EcoSafe®

Abbiamo il pallino di un futuro migliore

Servizi di consulenza, formazione
e comunicazione in ambito di sicurezza
sul lavoro, ambiente, sistemi di gestione
e di organizzazione aziendali.

ECOSAFE s.r.l. info@ecosafe.it
Torino Strada del Casas, 6/2 - 10090 Rosta, Torino - Italy - Tel +39 011 9541201 - Fax +39 011 0133199
Milano Via Giovanni XXIII, 2/A - 20866 Carnate (MB) - Italy - Tel +39 039 9630734
REA TO-101614 • P.IVA 08929640012 • Cap Soc € 10.000 i.v.