



POLITECNICO
MILANO 1863

SCHOOL OF MANAGEMENT



Come affrontare il GDPR e trasformarlo in opportunità?

Massimo Ficagna - Senior Advisor Osservatori Digital Innovation

Trento 16.11.2017



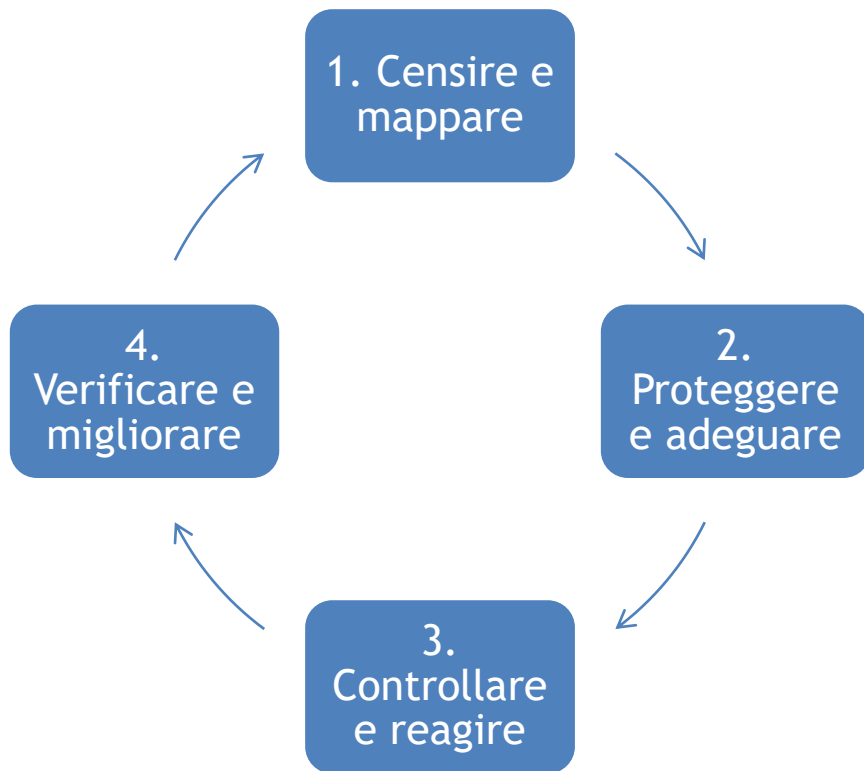
Non sono un legale ma un ingegnere.

Per una completa comprensione delle obbligazioni, dei ruoli e delle responsabilità relative al GDPR (Regolamento EU 2016/679) si raccomanda di far riferimento al testo ufficiale del Regolamento, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea, ed eventualmente di avvalersi di consulenza legale per la sua interpretazione*

* Disponibile al link:

<http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679>

Affrontare il GDPR in 4 fasi



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.

Fase 1: censire e mappare

Identifica i dati personali gestiti dalla tua organizzazione

Analizza le fonti di raccolta dati

Esempi tipici:

- *Attività di Marketing: registrazioni a newsletter, iscrizioni ad eventi, social registration, etc.*
- *Attività di vendita: e-commerce, anagrafiche/profilazione clienti,...*
- *Attività di recruiting: form di candidatura, servizi di head-hunting,...*
- ...

Analizza le basi di dati e gli archivi documentali



Fase 1: censire e mappare

Chiarisci le finalità per cui raccogli i dati

GDPR art. 13 e 14

Alla raccolta del consenso dal soggetto possessore dei dati personali, il titolare deve specificare (tra l'altro):

- le **finalità** del trattamento
- il **periodo di conservazione** dei dati (o i criteri corrispondenti)
- eventuali **logiche decisionali automatiche** basate sui dati raccolti
- l'eventuale **trasferimento dei dati in Paesi terzi** (extra EU)

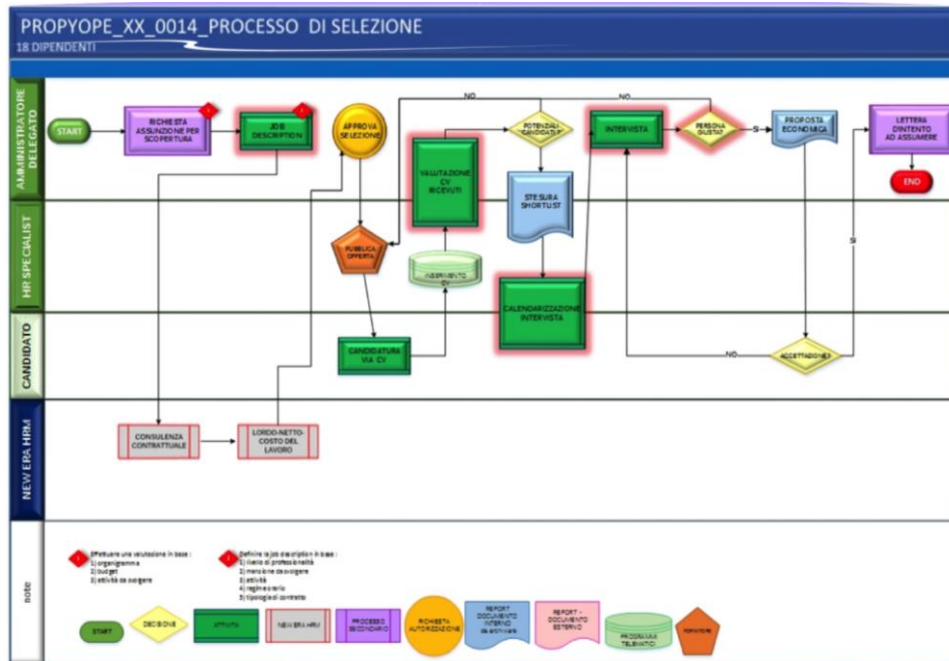


Fase 1: censire e mappare

Mappa i processi di trattamento

- Attività di trattamento interne:
 - raccolta,
 - elaborazione primaria/secondaria,
 - archiviazione,
 - eliminazione
- Ruoli/attori coinvolti
- Applicazioni utilizzate
- Archivi
- Trasferimenti a terze parti e trattamenti esterni

L'analisi dei dati personali contenuti nelle basi di dati può complementare l'analisi dei processi di trattamento



Fase 1: censire e mappare

Valuta se nominare il DPO

GDPR art. 37, 38, 39

È necessario nominare un **Responsabile della Protezione dei Dati (DPO = Data Protection Officer)** se:

- il trattamento è effettuato da un'autorità pubblica o da un **organismo pubblico**, eccetto autorità giurisdizionali nell'esercizio delle loro funzioni;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono in:
 - trattamenti che richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**; e/o
 - **trattamento, su larga scala, di categorie particolari di dati personali** (dati «sensibili» specificati all'art. 9 o dati relativi a condanne penali e a reati, art. 10).

È comunque possibile nominare un DPO anche ove non esplicitamente richiesto.

Il DPO può essere sia interno che esterno.



Fase 2. Proteggere e adeguare

Identifica i rischi e valuta gli impatti

La valutazione formale dei rischi e degli impatti (DPIA - Data Protection Impact Assessment) non è obbligatoria per tutte le tipologie di trattamenti (ma può essere comunque opportuna).

Una singola valutazione può coprire più trattamenti analoghi.

Nel valutare i rischi si tiene conto in particolare (ma non solo) di:

- distruzione,
- perdita,
- alterazione,
- accesso non autorizzato,
- divulgazione non autorizzata,

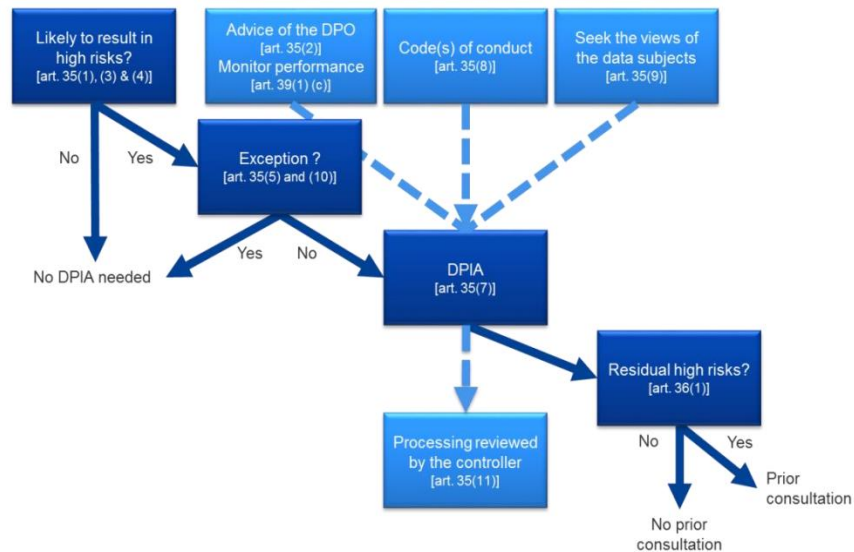
in modo accidentale o illegale, relativamente ai dati personali trasmessi, conservati o comunque trattati.

Per valutare l'impatto si possono usare metodologie standard quali ISO 31000:2009 e ISO/IEC 29134

Per maggiori dettagli, si rimanda alle linee guida del Working Party art. 29:

http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

GDPR art. 32 e 35



Fase 2. Proteggere e adeguare

Adotta le contromisure opportune

GDPR art. 32 e 35

Aspetti di sicurezza da considerare:

- **Controllo accessi:** autenticazione e autorizzazione
- **Protezione dei dati:** cifratura e pseudonimizzazione
- **Disponibilità dei dati:** resilienza e disaster recovery

*Non esistono più le misure minime di sicurezza...
e non esiste la sicurezza assoluta!*

*Si tratta di scegliere le misure di sicurezza
«ragionevoli» in funzione del contesto
aziendale*

Il GDPR definisce i contenuti minimi del DPIA:

- *descrizione delle operazioni di trattamento e degli scopi del trattamento;*
- *valutazione dell'effettiva necessità e proporzionalità del trattamento;*
- *valutazione dei rischi, rispetto ai diritti e alle libertà dei soggetti del trattamento;*
- *misure adottate per:*
 - *mitigare i rischi;*
 - *dimostrare la conformità con il Regolamento GDPR*

Fase 2. Proteggere e adeguare

Predisponi le procedure necessarie

GDPR art. 15 → 22

Devono essere predisposte le procedure e gli eventuali strumenti informatici per gestire i seguenti diritti dei soggetti del trattamento:

- informazione (oltre al consenso, qualora i dati non siano raccolti direttamente dall'interessato)
- accesso ai dati
- oblio (cancellazione)
- rettifica dei dati
- opposizione al trattamento
- limitazione del trattamento
- portabilità dei dati
- revisione delle decisioni prese da processi automatici di trattamento

Information



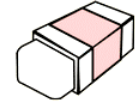
Access



Rectification



Erasure



Restriction



Portability



Objection



Revision of automation



Fase 3. Controllare e reagire

Preparati a gestire il peggio!

GDPR art. 33 e 34

Per essere pronti ad affrontare eventuali situazione di violazioni alla privacy (accidentali o intenzionali), è opportuno:

- **Tracciare** preventivamente tutte le operazioni di trattamento
- Predisporre strumenti per:
 - **monitorare** la sicurezza
 - **generare alert** in caso di violazioni
- Predisporre procedure dedicate a **gestire la notifica all'autorità di controllo (Garante)** di eventuali violazioni degli standard di sicurezza adottati



Per supportare l'analisi forense, in caso di violazioni



Per reagire tempestivamente, attuando le contromisure più opportune



Per valutare se la violazione comporta dei rischi in relazione ai diritti e alle libertà degli interessati e rispettare i tempi massimi (72h) di notifica all'autorità di controllo e, nei casi di alto rischio, anche ai diretti interessati

Fase 4. Verificare e migliorare

Aggiorna continuamente

Nel tempo:

- cambiano e si espandono le tipologie di dati raccolti e i trattamenti necessari;
- il sistema informativo aziendale evolve;
- nascono nuove tecniche di attacco e minacce alla sicurezza informatica.

Il GDPR non deve essere visto come un progetto una-tantum, ma come un **processo continuativo**.

E' necessario predisporre **modalità sistematiche di revisione/aggiornamento** di procedure, soluzioni tecniche e documentazione per il trattamento corretto e sicuro dei dati personali.

GDPR artt. 25, 40, 42

Per le nuove applicazioni / sistemi devono essere considerati i principi di:

- **Privacy by Design**
- **Privacy by Default**

In futuro, la conformità al GDPR potrà essere dimostrata mediante l'adesione a:

- *un codice di condotta approvato*
- *un meccanismo di certificazione approvato*

NOTA: attualmente non ancora disponibili!

Vuoi trasformare il GDPR in un'occasione per migliorare il rapporto con i tuoi clienti / utenti?



- *Comunica in modo particolarmente chiaro e trasparente le finalità dei trattamenti (evidenziando i benefici per gli interessati)*
- *Rendi molto facile agli interessati l'esercizio dei loro diritti, con funzionalità self-service che permettano di consultare ed esportare i propri dati, visualizzare ed eventualmente modificare i consensi lasciati nel tempo o richiedere la cancellazione*