Adeguamento al GDPR

Versione 0.1

Premessa

Il Regolamento generale per la protezione dei dati personali n. 2016/679 (*General Data Protection Regulation* o GDPR) è la normativa di riforma della legislazione europea in materia di protezione dei dati personali. Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016, ma la sua attuazione avverrà a distanza di due anni, quindi a partire dal 25 maggio 2018.

Il Regolamento pone con particolare enfasi l'accento sulla responsabilizzazione (*accountability*) del Titolare e dei Responsabili del trattamento, che si deve concretizzare nell'adozione di comportamenti proattivi a dimostrazione della concreta (e non meramente formale) adozione del Regolamento. In particolare il legislatore evidenzia la necessità di attuare misure di tutela e garanzia dei dati trattati con un approccio del tutto nuovo, che demanda ai Titolari il compito di decidere **autonomamente** le modalità e i limiti del trattamento dei dati alla luce dei principi fondamentali indicati nel Regolamento:

- principio "*privacy by design*", in base al quale i prodotti e i servizi dovranno essere progettati fin dall'inizio in modo da tutelare la privacy degli utenti;
- minimizzazione del *rischio* del trattamento, inteso come valutazione e minimizzazione dell'impatto negativo sulle libertà e i diritti degli Interessati.

L'approccio del GDPR è una evoluzione molto significativa della precedente normativa: si tende a realizzare un approccio maggiormente basato sulla valutazione del rischio (*risk based*), con la quale si determina *ex ante* l'entità della responsabilità del Titolare o del Responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti.

Un approccio *risk based* ha le evidenti conseguenze di richiedere degli obblighi che possono andare oltre la mera presunta conformità alla norma e di assicurare maggiore flessibilità al mutare delle esigenze e degli strumenti tecnologici, ma ha anche lo svantaggio di delegare all'ente la valutazione del rischio, rendendo più difficili le contestazioni in caso di violazioni.

Metodologia del Comune di Fagnano Olona

In attuazione del principio della maggiore responsabilizzazione (*accountability*), il Comune di Fagnano Olona ha intrapreso un percorso di adeguamento che consenta di transitare in modo efficace dal rispetto della precedente normativa alla realizzazione e al mantenimento della piena conformità in tema di tutela della privacy prevista dal GDPR.

Considerando che attualmente il Comune è sostanzialmente conforme alla precedente normativa, il processo di adeguamento ha l'obiettivo principale di modificare le misure in atto alla luce delle novità introdotte dal GDPR.

In particolare, le principali novità introdotte dal GDPR riguardano:

1. l'attivazione del nuovo ruolo di Responsabile della Protezione dati (DPO) e le conseguenti modifiche funzionali ai ruoli di Titolare e Responsabile del trattamento;
2. la formazione del personale, che dovrà essere più specifica e capillare rispetto al passato;
3. la redazione di nuovi documenti, quali il Registro dei trattamenti, la valutazione d'impatto, il registro dei *data breach* e l'analisi dei rischi.

Ovviamente, si coglierà l'occasione per attivare i processi necessari per assicurare che i nuovi trattamenti che dovessero essere acquisiti nel futuro vengano realizzati nel pieno rispetto dei suddetti principi del *privacy by design* e di minimizzazione del rischio. Al raggiungimento di questi obiettivi sono dedicate le due attività aggiuntive di Gap analisys e Adeguamento delle misure di sicurezza.

In questo contesto generale, è stato attivato lo specifico processo aziendale descritto in questo documento: tale processo è, al momento, costituito dalle seguenti Attività:

1. Attività 01 - Rilevazioni preliminari
2. Attività 02 – Struttura organizzativa e funzionale
3. Attività 03 – Formazione
4. Attività 04 – Documentazione *ex GDPR*
5. Attività 05 - Gap analisys
6. Attività 06 – Adeguamento misure di sicurezza

A tali attività, verranno successivamente aggiunti tutti i processi ritenuti necessari per mantenere nel tempo la desiderata conformità al GDPR .

Il presente documento, quindi, verrà aggiornato in modo continuo nel tempo, al procedere delle attività e tenendo conto delle risultanze delle analisi effettuate.

Attività 01 - Rilevazioni preliminari

Devono essere svolte alcune attività preliminari alla definizione della strategia di adeguamento al nuovo GDPR:

1. Ricognizione dei trattamenti in essere. Tale ricognizione deve riguardare sia i trattamenti che riguardano dati *interni*, intesi come quei Trattamenti di cui il Comune di Fagnano Olona è Titolare (come, ad es: i dati per la gestione amministrativa e del personale), sia i trattamenti che vengono svolti per conto terzi (quando il Titolare non è il Comune di Fagnano Olona);
2. Acquisizione e analisi della documentazione esistente dei suddetti trattamenti. Dall'analisi della documentazione si dovranno individuare le caratteristiche principali dei Trattamenti, come, ad esempio:
    a. Struttura privacy (Legittimità normativa, Titolare, Responsabili, Incaricati)
    b. Tipologia di Interessati
    c. Tipologia del Trattamento dei dati
    d. Misure di sicurezza adottate

In Figura 1 è riportato il processo che realizza tali attività;

1. La Funzione Privacy inizia il processo richiedendo formalmente a vari responsabili di Settore e Servizi di verificare la natura dei trattamenti di dati che vengono svolti sotto la loro responsabilità.
2. I Destinatari della richiesta forniscono le informazioni entro un tempo prefissato, includendo, se disponibile, la documentazione rilevante per gli obiettivi della presente attività;
3. La Funzione Privacy analizza e verifica le informazioni ricevute, con lo scopo di evidenziare eventuali aspetti problematici

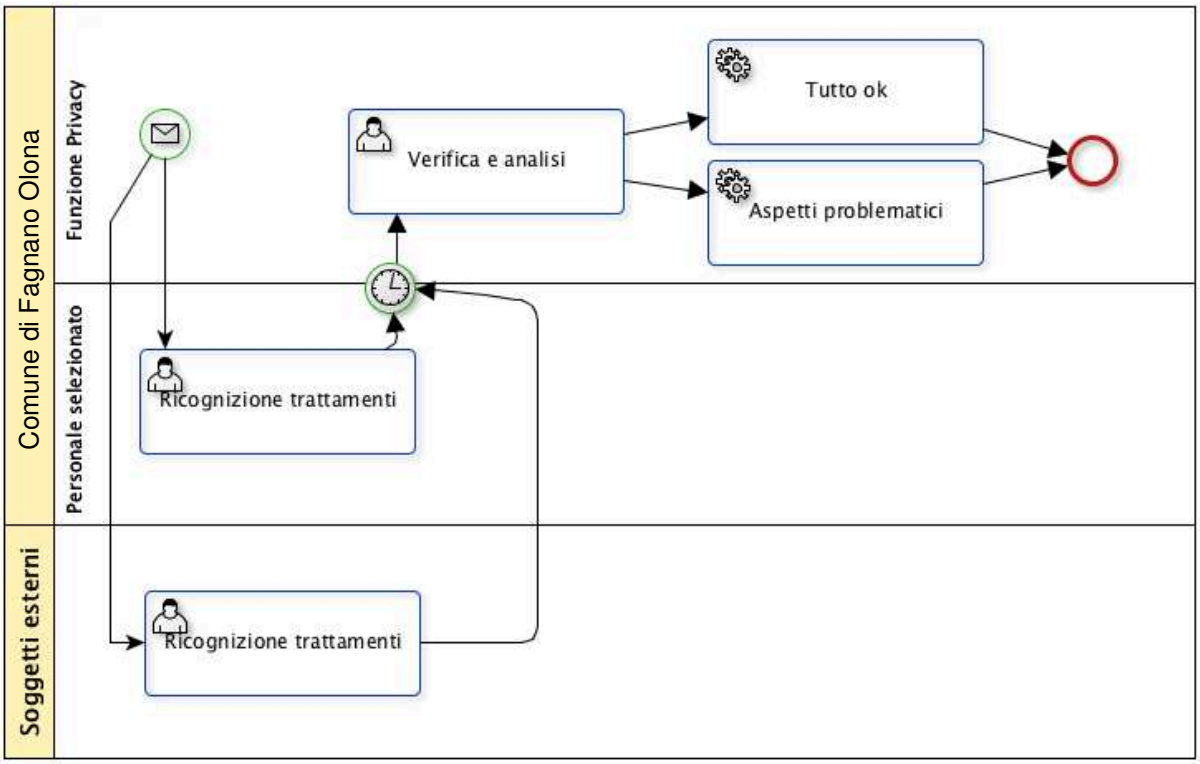

Figura 1: Processo di rilevazione dei Trattamenti in essere

Attività 02 – Struttura organizzativa e funzionale

Il GDPR richiede una struttura organizzativa parzialmente differente rispetto alla precedente normativa introducendo, in particolare, la funzione del Responsabile Protezione Dati o *Data protection Officer* (DPO).

Il ruolo di DPO è descritto in:

- GDPR – capo IV – Titolare del trattamento e responsabile del trattamento – Sezione 4 – Responsabile della protezione dei dati:
  - Articolo 37 - Designazione del responsabile della protezione dei dati
  - Articolo 38 - Posizione del responsabile della protezione dei dati
  - Articolo 39 - Compiti del responsabile della protezione dei dati
- Linee-guida sui responsabili della protezione dei dati (DPO) (GRUPPO DI LAVORO ART. 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI)

La nuova struttura organizzativa e funzionale deve essere costituita in modo formale, individuando, in particolare, le persone per i ruoli di Titolare, Responsabili esterni, organizzazione interna.

In Figura 2 è riportato il processo che realizza l'Attività:

- Il Titolare individua i nuovi ruoli e le persone che ricopriranno tali ruoli, comunicando le decisioni alle persone interessate
- Le persone accettano formalmente l'incarico
- In caso di soggetti esterni, si veda il contratto e, in caso di necessità, lo stesso verrà integrato.

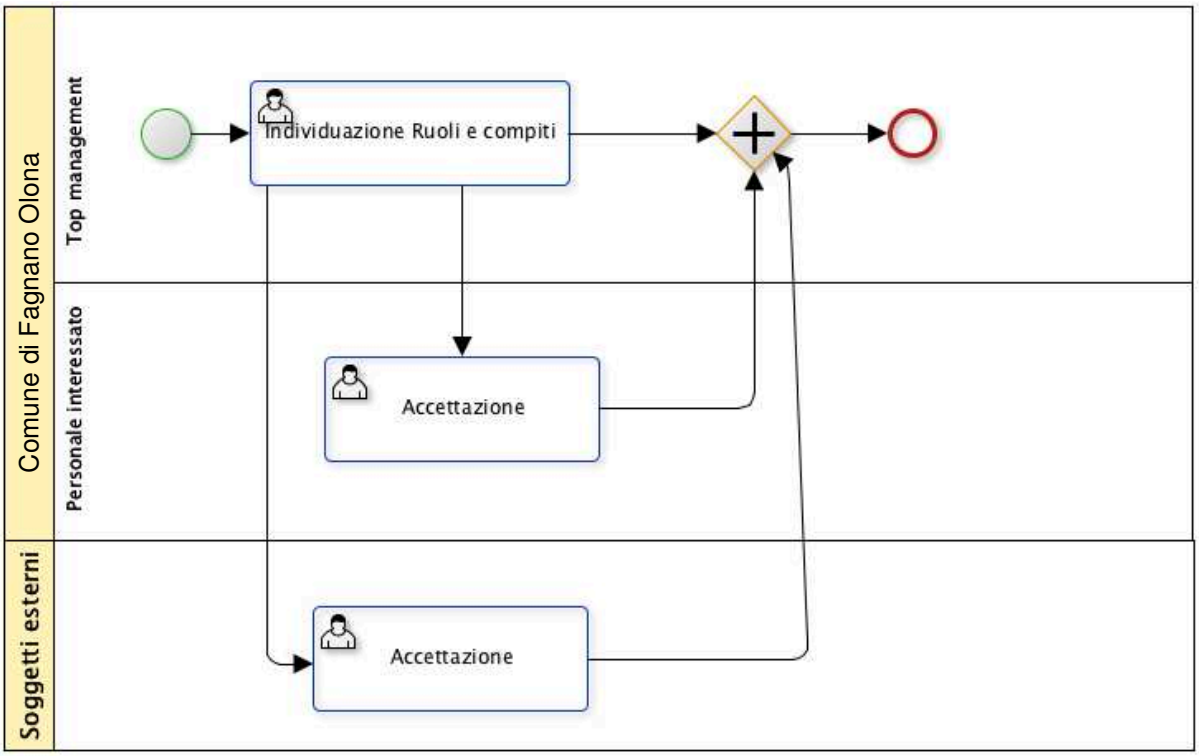

Figura 2: Processo di definizione nuova struttura funzionale

Attività 03 - Formazione

Il GDPR prevede una costante e aggiornata formazione del personale. In particolare, l'art. 39 del Regolamento prevede, tra i vari compiti affidati al DPO, quello di: "informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati".

In Figura 3 è riportato il processo di formazione, la cui organizzazione ed erogazione è in capo al Titolare e/o al DPO. Il processo deve essere inteso come un processo continuativo nel tempo.

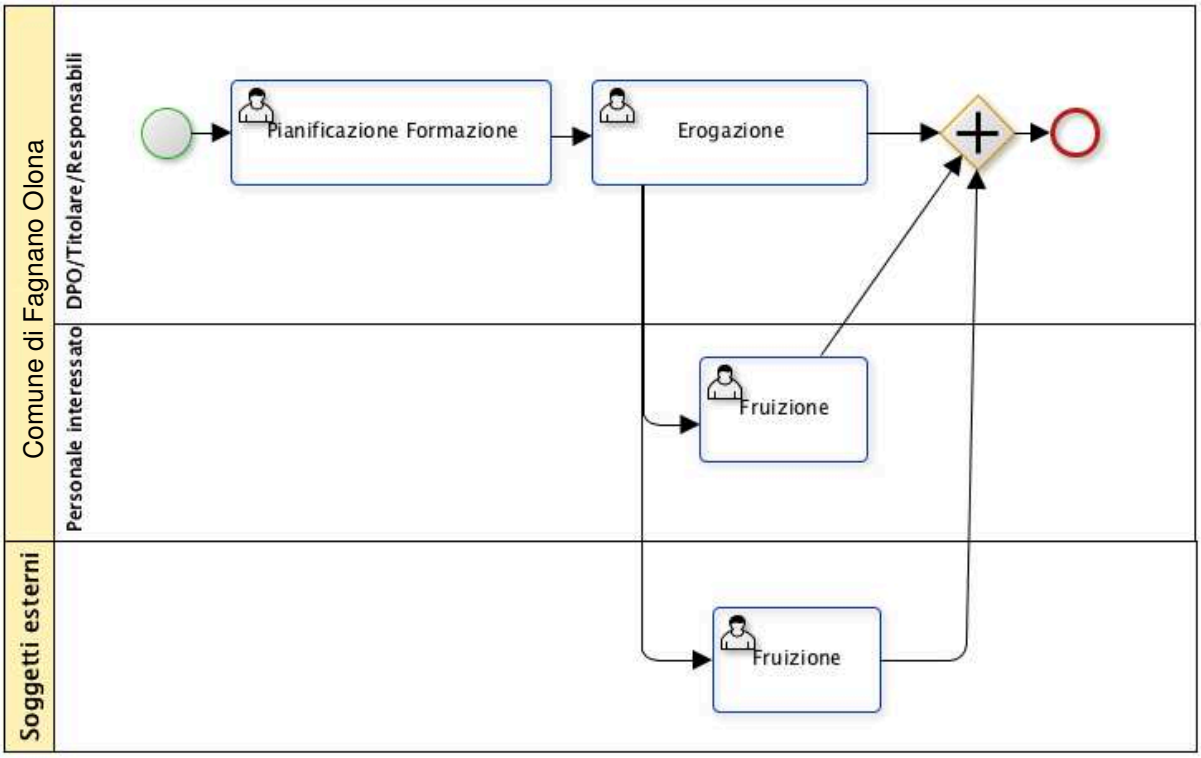

Figura 3: Processo di formazione del personale

Attività 04 – Documentazione *ex GDPR*

Il GDPR prevede la redazione di nuova documentazione rispetto alla normativa previgente: ad ogni "documento" corrisponde una attività finalizzata a realizzare il principio generale dell'*accountability*.

In particolare, si dovranno redigere i seguenti documenti:

- Registro dei Trattamenti. L'art. 30 del GDPR recita:

  1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
  a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
  b) le finalità del trattamento;
  c) una descrizione delle categorie di interessati e delle categorie di dati personali;
  d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
  e) ove applicabile, 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;
  f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
  2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
  a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
  b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
  c) ove applicabile, 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;
  d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
  3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
  4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
  5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.
- Misure di sicurezza. Tale documentazione dovrà essere redatta considerando le disposizioni contenute in GDPR, Sezione 2, Articolo 32: Sicurezza del trattamento, Art. 24: Responsabilità del titolare del trattamento, Art. 25: Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (C75-C78)
- Valutazione d'impatto (Data Protection impact Analisys: DPIA). Tale documentazione dovrà essere redatta considerando:

- GDPR Sezione 3 - Valutazione d'impatto sulla protezione dei dati e consultazione preventiva
  - Art. 35: Valutazione d'impatto sulla protezione dei dati (C84, C89-C93, C95)
  - Art. 36: Consultazione preventiva (C94-C96)
- Linee-guida (WP29) concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679

- Registro dei *Data breach*. Il GDPR impone la redazione di un registro degli incidenti informatici, tra i quali potrebbero essere individuati incidenti che hanno un particolare impatto sul trattamento dei dati personali (*Data Breach*). Tale documentazione dovrà essere redatta considerando GDPR
  - Articolo 33: Notifica di una violazione dei dati personali all'autorità di controllo
  - Articolo 34: Comunicazione di una violazione dei dati personali all'interessato Guidelines on Personal data breach notification under Regulation 2016/679.

In Figura 4 è riportato il processo di redazione dei suddetti documenti

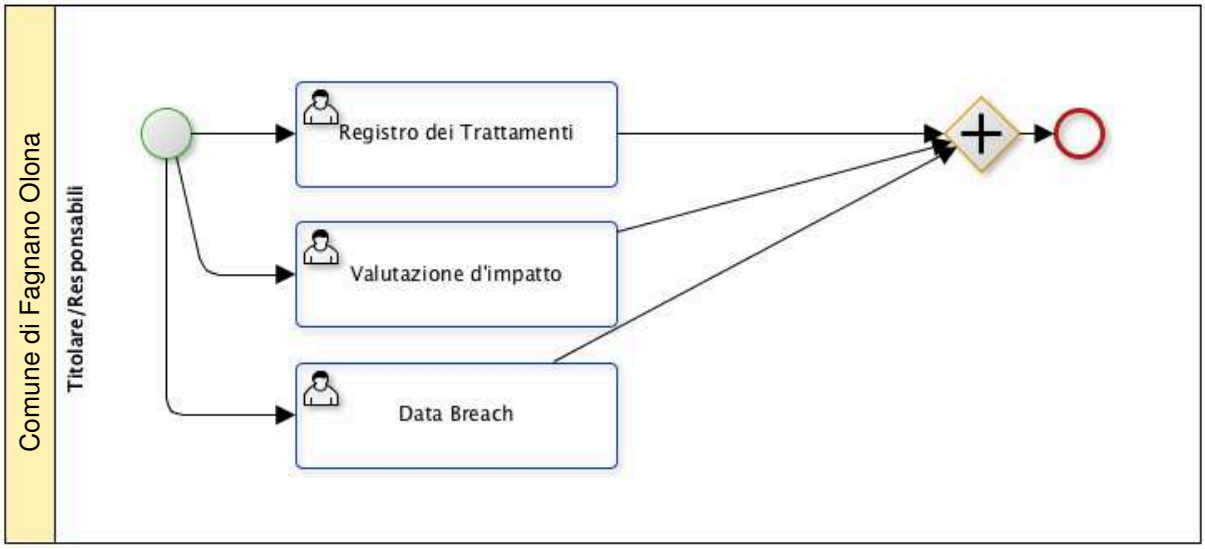

Figura 4: Processo di redazione di documentazione specifica

Attività 05 - Gap analisys

Sulle basi delle risultanze delle attività precedenti, presumibilmente, occorrerà svolgere una *Gap Analisys* tra le misure di sicurezza esistenti e quelle necessarie per assicurare la *compliance* con il GDPR.

Attività 06 – Adeguamento misure di sicurezza

Sulle basi delle risultanze della *Gap Analisys*, sarà, presumibilmente, necessario realizzare un adeguamento delle misure di sicurezza dei Trattamenti in modo da completare l'adeguamento a quanto previsto dal GDPR.

Tempistica

In relazione alle attività sopra elencate, si stabilisce di procedere, anche a mezzo di affidamento esterno, entro il 25/05/2018 per le attività 1, 2 e 4.

È evidente che, per le altre attività, sarà necessario un tempo maggiore, tenuto conto che l'attuale organizzazione dell'Ente in tema di privacy risulta sostanzialmente in linea con la normativa previgente, ma si deve effettuare un puntuale lavoro di analisi per valutare le eventuali necessità di adeguamento al GDPR.