Tutorial GDPR: il Modello organizzativo

Sergio Duretti, Direttore Integrazioni Digitali - RPD per la PAL dell'Emilia, le ASP e i Consorzi di Bonifica

Argomenti

1. Le ragioni del modello
2. Gli attori del modello
3. il Titolare del trattamento
4. i Soggetti delegati attuatori
5. i Responsabili del trattamento
6. gli Incaricati
7. il Responsabile della Protezione dei dati
8. i Sistemi informativi
9. il Responsabile competente in materia di sistemi informativi
10. il Gruppo dei referenti privacy

Le ragioni del modello

1. Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio europeo del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito anche solo "Regolamento") detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici **obblighi ed adempimenti** a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni.
2. Nel Modello organizzativo ciascun Ente definisce il **proprio ambito** di titolarità, delega a Dirigenti e Incaricati di P.O., ciascuno per il proprio ambito di competenza, l'attuazione degli adempimenti previsti dalla normativa, indica i compiti assegnati al RPD designato e definisce i criteri generali da rispettare nell'individuazione dei soggetti autorizzati a compiere le operazioni di trattamento, delineando il complessivo ambito delle responsabilità.
3. Particolare attenzione viene prestata alle responsabilità relative alla gestione dei **sistemi informativi** dell'Ente.

Gli attori del modello

Il Regolamento europeo individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

- Il **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- Il **Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- Il **Responsabile della Protezione dei Dati** (di seguito anche RPD): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;
- **Persone autorizzate al trattamento** dei dati personali sotto l'autorità diretta del titolare o responsabile: figura che si desume implicitamente dalla definizione di "terzo" di cui al n. 10 del comma 1 art. 4 del Regolamento.

il Titolare del trattamento

I **principali compiti** previsti per il Titolare del trattamento sono:

1. Adottare, nelle forme previste dal proprio ordinamento, gli interventi normativi necessari, anche con riferimento alle disposizioni del Codice per la protezione dei dati personali oggetto di adeguamento al Regolamento;
2. Designare il Responsabile della Protezione dei Dati;
3. Designare i soggetti delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
4. Effettuare, a mezzo dei servizi competenti, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compresi i profili relativi alla sicurezza informatica, in collaborazione con il RPD designato;
5. Istruire i soggetti autorizzati al trattamento dei dati personali.

i Soggetti delegati attuatori / 1

I soggetti delegati attuatori sono le **persone designate dal Titolare del trattamento** all'interno del'Ente e a cui sono **delegati** i seguenti **principali compiti**:

1. Adottare soluzioni di privacy "by design" e "by default", ossia configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti dell'interessato,
2. Predisporre il modello di informativa relativo al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento;
3. Predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
4. Disporre l'adozione dei provvedimenti imposti dal Garante;
5. Collaborare con il RPD al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnati;
6. Adottare, se necessario, specifici Disciplinari tecnici per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali;
7. Garantire al Responsabile dei sistemi informativi e al RPD i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;

i Soggetti delegati attuatori / 2

8. Designare l'Amministratore di sistema in aderenza alle norme vigenti in materia;;
9. Effettuare la preventiva valutazione d'impatto ove necessaria ai sensi dell'art. 35 del Regolamento;
10. Consultare il Garante, in aderenza all'art. 36 del Regolamento nei casi in cui la valutazione d'impatto a norma dell'art. 35 indichi che il trattamento presenta un rischio residuale elevato;
11. Richiamare obbligatoriamente nei contratti di sviluppo di software e piattaforme, la policy in materia di sviluppo delle applicazioni, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'Ente di risoluzione del contratto;
12. Designare i Responsabili del trattamento;
13. Tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;
14. Individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;

i Responsabili del trattamento

Sono designati Responsabili del trattamento di dati personali **i soggetti esterni** all'Amministrazione che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare.

Pertanto, qualora occorra affidare un incarico che preveda trattamento di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinchè lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale.

il Responsabile della protezione dei dati /1

Il Regolamento 679/2016 prevede **l'obbligo per gli Enti pubblici** di designare il Responsabile della protezione dei dati (RPD).

Sono di seguito indicati i **principali compiti** del RPD:

- Informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con il supporto del gruppo dei referenti privacy dell'Ente;
- Sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell'Ente in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- Coopera con il Garante per la protezione dei dati personali;
- Funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
- Partecipa allo svolgimento delle verifiche di sicurezza svolte da chi ha la responsabilità dei sistemi informativi o ne richiede di specifiche;

il Responsabile della protezione dei dati /2

- Partecipa alla gestione conseguente ad eventuali incidenti di sicurezza nelle modalità previste da specifica policy dell'Ente;
- Promuove e cura la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;
- Formula gli indirizzi per la realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento;
- Fornisce i pareri obbligatori e facoltativi richiesti secondo quanto specificato di seguito.

Pareri Responsabile della protezione dei dati/1

Pareri obbligatori

Devono essere **obbligatoriamente** richiesti pareri in ordine a:

- Individuazione delle misure che abbiano significativo impatto sulla protezione dei dati personali che l'Ente intende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente, anche a seguito di incidenti di sicurezza o analisi dei rischi;
- Adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici con impatto sulla sicurezza delle informazioni;
- Individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
- Incidenti relativi alla sicurezza.

Pareri Responsabile della protezione dei dati/2

Pareri facoltativi

Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:

- Progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza ai principi della privacy by design e by default;
- Eventuale valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento;
- Valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5 bis e, in via generale, del Regolamento n. 679/2016;
- Opposizione formulata dai controinteressati nella misura incui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Accesso civico/1

Il contesto

E' necessario disciplinare l'interazione tra il RPD, le Strutture dell'Ente e il Responsabile per la prevenzione della corruzione e trasparenza (R.P.C.T.).

Il D.Lgs. n. 97/2016, di modifica del D.Lgs. n. 33/2013, ha introdotto l'istituto dell'accesso civico "Generalizzato", che attribuisce a Chiunque" il "diritto di accedere ai dati, ai documenti e alle informazioni detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione."

L'esercizio di tale diritto soggiace a limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'art. 5 bis del D.Lgs. n. 33/2013.

L'art. 5, comma 5, del D.Lgs. n. 33/2013 prevede che, per ciascuna domanda di accesso generalizzato, l'amministrazione debba verificare l'eventuale esistenza di controinteressati, eccetto i casi in cui la richiesta di accesso civico abbia ad oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria.

Accesso civico/2

Il RPD **funge da supporto** ai Servizi competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti le richieste di accesso civico generalizzato.

Il RPD funge altresì da supporto al R.P.C.T. nei casi di riesame di istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali.

Il RPD, inoltre, su richiesta dei Servizi competenti, esprime parere in ordine alla valutazione dell'eventuale pregiudizio che l'accesso potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5 bis e, in via generale, del Regolamento n. 679 del 2016.

Il RPD, su richiesta dei Servizi competenti, formula il proprio parere, entro tre giorni, in ordine all'opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Sulla scorta di tale parere i Servizi competenti sulle singole richieste di accesso effettueranno il bilanciamento tra gli interessi asseritamente lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.

gli Incaricati

Gli incaricati sono tutti coloro che sono **autorizzati al compimento delle operazioni dei dati dai soggetti delegati attuatori** secondo le seguenti istruzioni generali:

- Sono trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- Sono verificati legittimità e correttezza dei trattamenti, verificando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

Sono autorizzati al trattamento dei dati tutti i soggetti, dipendenti e collaboratori a qualsiasi titolo, che operano sotto la diretta autorità del Titolare o dei soggetti delegati attuatori.

Tali soggetti devono essere da questi formalmente autorizzati.

Gli incaricati sono designati:

- Tramite individuazione nominativa delle persone fisiche specificando, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare;
- Tramite assegnazione funzionale della persona fisica all'unità organizzativa qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità.
- Le istruzioni impartite agli incaricati del trattamento devono essere allegate alla designazione scritta dell'incaricato.

i Sistemi informativi /1

Il Servizio competente in materia di sistemi informativi, ovvero di sicurezza informatica, svolge un **ruolo di supporto al RPD** in tema di risorse strumentali e di competenze svolgendo i compiti di seguito specificati:

- Individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente. Tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo obbligatorio del RPD , come ad esempio per la redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e per la redazione ed aggiornamento dei disciplinari tecnici trasversali;
- Condivide le evidenze dell'analisi dei rischi con il RPD, il quale fornisce parere obbligatorio sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;

i Sistemi informativi /2

- promuove l'informazione di tutto il personale dell'Ente in materia di sicurezza informatica, attraverso un piano di comunicazione e divulgazione all'interno dell'Ente, coordinandosi con le azioni promosse dal RPD.
- svolge verifiche sulla puntuale osservanza della normativa e delle policy aziendali in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del RPD e realizza le verifiche specifiche richieste dallo stesso;
- Provvede, ogni qualvolta venga avvertito un problema di sicurezza a:
  - Svolgere i compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del RPD;
  - Individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del RPD;
  - Segnalare al Titolare del trattamento o al Soggetto attuatore delegato le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali;

il Responsabile dei sistemi informativi

Al Responsabile competente in materia di sistemi informativi spetta:

- l'adozione di policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario;
- la segnalazione al Titolare del trattamento o al soggetto attuatore delegato delle violazioni dei dati personali su sistemi elettronici ai fini della notifica ai sensi dell'art. 33 del Regolamento, al garante per la protezione dei dati personali.

il Gruppo referenti privacy

La costituzione di un gruppo permanente di referenti privacy, formato dai soggetti individuati quali responsabili dell'Ente, che assicuri un presidio per gli adempimenti continuativi, lo studio e l'approfondimento degli aspetti normativi, organizzativi e procedurali, costituisce attuazione dei principi di informazione e sensibilizzazione del Regolamento europeo n. 679/2016

Il Gruppo dei referenti ha i seguenti **principali compiti**:

- attuare, per le strutture di appartenenza, le misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Ente, anche a seguito ad analisi ed approfondimenti in seno al Gruppo dei referenti;
- coordinare il puntuale aggiornamento della designazione dell'Amministratore di Sistema e la costante verifica dei privilegi assegnati allo stesso;
- effettuare la ricognizione costante, a mezzo del Registro, dei trattamenti di dati personali effettuati dalle strutture di appartenenza, servendosi di risorse e competenze messe all'uopo a disposizione;
- supportare le verifiche di sicurezza svolte dal Servizio "Sistemi Informativi" e/o dal RPD;
- trasmettere per il tramite del Referente dell'Ente, le richieste di parere al RPD di propria afferenza nei casi e con le modalità previsti dal presente documento.

Informazioni e contatti

gdpr@lepida.it