A.S.L. TO4
Azienda Sanitaria Locale
di Ciriè, Chivasso e Ivrea

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

PROCEDURA
PER LA
COMPILAZIONE E LA GESTIONE DEL
REGISTRO DEI TRATTAMENTI

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

Riferimenti:

- Reg. (UE) 2016/679 (GDPR) 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;
- D.Lgs. 196/2003 e s.m.i. "Codice in materia di protezione dei dati personali" così come novellato dal D.Lgs. 101/2018;
- D.Lgs. 101/2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 (norme transitorie);
- FAQ sul registro delle attività di trattamento dell'Autorità di controllo dell'8 ottobre 2018;
- CNIL (Autorità di controllo francese), linee guida "Il registro delle attività di trattamento";
- DPA (Autorità di controllo belga), linee guida "Registro delle attività di trattamento";
- WP 248 "Linee guida in materia di valutazione d'impatto sulla protezione dei dati";
- WP 259 "Linee guida sul consenso ai sensi del regolamento (UE) 2016/679";
- Manuale RPD - Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e para pubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea - T4DATA.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

INTRODUZIONE

Premessa

L'art. 30 del GDPR introduce l'obbligo della tenuta del registro dei trattamenti, ovvero uno strumento che consente di tenere traccia di tutte le operazioni di trattamento di dati personali effettuate all'interno dell'Ente.

Per quanto attiene ai soggetti obbligati alla tenuta del registro dei trattamenti, deve precisarsi che:

- l'art. 30 par. 1 disciplina il registro dei trattamenti del Titolare, stabilendo che ogni Titolare del trattamento e, ove applicabile, il suo rappresentante, tengono un registro delle attività di trattamento svolte sotto la propria responsabilità;
- l'art. 30 par. 2 disciplina invece il registro dei trattamenti del responsabile, stabilendo che 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.

I due registri presentano delle differenze dal punto di vista contenutistico, avendo il registro del Titolare del trattamento una portata più ampia che si estende, ad esempio, all'indicazione delle finalità del trattamento, delle categorie di dati personali etc.

Scopo

Obiettivo di questo documento è quello di illustrare i passi da compiere per effettuare una corretta compilazione e gestione del Registro dei trattamenti. Redigere e mantenere un Registro dei trattamenti completo e aggiornato rappresenta uno strumento per dimostrare la propria Accountability (Conoscenza, Competenza e Responsabilità) e per evitare pesanti sanzione amministrative pecuniarie che possono arrivare fino a 10 milioni di euro e al 2% del fatturato mondiale annuo.

Area di applicazione

La procedura è applicata a tutte le strutture aziendali che effettuano trattamenti di dati personali.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

Acronimi e abbreviazioni

Nel documento sono utilizzati i seguenti acronimi (e/o abbreviazioni):

- *GDPR* General Data Protection Regulation
- *WP* Working Party
- *DPIA* Data Protection Impact Assessment
- *TEAM DEL DPO* Data Protection Officer
- *ADS* Amministratore di Sistema
- *Delegato* Definizione come da Delibera del D.G. numero 587 del 15/05/2019
- *Ufficio Privacy* presso S.S. Legale e Assicurazioni
- *Gruppo di lavoro Privacy* Gruppo costituito come da Delibera del D.G. numero 457 del 13/04/2018 e s.m.i.
- *Risk Owner come gestore del rischio (clinico e informatico)*

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

1. DESCRIZIONE PROCEDURA

1.1. Attivazione

La presente procedura viene attivata:

- Con una segnalazione al D.P.O. aziendale o, in alternativa, all'Ufficio Privacy aziendale da parte di uno o più Delegati aziendali al trattamento dei dati, qualora ravvisino la necessità di:
  - Inserire uno o più trattamenti *ex novo* all'interno del registro dei trattamenti come conseguenza, ad esempio, dell'avvio di nuove attività o come conseguenza dell'inizio di un nuovo servizio che prevedano il trattamento di dati;
  - Rivedere le informazioni relative a uno o più trattamenti già censiti nel Registro dei trattamenti (es. variazione delle finalità del trattamento, variazione del servizio/attività, aggiornare/variare uno o più supporti utilizzati per eseguire il trattamento o dismettere gli stessi perché obsoleti etc.);
  - Aggiornare le informazioni già censite a seguito di un cambio organizzativo;
  - Archiviare uno o più trattamenti, come conseguenza ad esempio, della cessazione di una o più attività che prevedono il trattamento di dati personali. In questo modo si ha uno storico del Registro;
- Con una specifica richiesta dell'Ufficio Privacy o del Gruppo di Lavoro Privacy aziendali, avanzata ai Delegati durante l'attività di revisione del Registro dei trattamenti con una cadenza semestrale, per raccogliere eventuali aggiornamenti;
- Con una segnalazione del Team del DPO Aziendale che ha ravvisato una o più non conformità durante l'attività di *audit*;
- Con una segnalazione del Team del DPO Aziendale a seguito di un'attività ispettiva dell'Autorità Garante per la protezione dei dati personali che ha ravvisato una o più irregolarità tra quanto censito nel Registro dei trattamenti e i trattamenti effettivamente eseguiti dal Titolare del trattamento.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

1.2. Input e Output

Le informazioni che entrano in input alla procedura nei vari passi sono:

- *Input 1: informazioni da organigramma aziendale (struttura dell'organizzazione aziendale), o da scheda di Registro già esistente, nel caso in cui si debba variare o aggiornare un trattamento.*
- *Input 2: dati forniti dai Delegati o loro incaricati rispetto ad ogni trattamento effettuato dalla propria Struttura (ad es: norme, fornitori di beni e servizi, base giuridica, etc.).*

Le informazioni che escono quali output della procedura nei vari passi sono:

- *Output 1: adempimenti di legge (art. 30, par. 1 GDPR).*
- *Output 2: scheda di Registro completa relativa al trattamento da inserire, integrare o aggiornare.*
- *Output 3: analisi dei rischi.*
- *Output 4: possibile valutazione d'impatto.*
- *Output 5: redazione ed aggiornamento di ogni necessaria informativa*
- *Output 6: ulteriori adempimenti.*

1.3. Passi procedurali

1.3.1. Costruire il Registro dei trattamenti

Il paragrafo numero 5 dell'art. 30 del GDPR specifica che la tenuta del Registro dei trattamenti è obbligatoria per le imprese o organizzazioni con più di 250 dipendenti o con meno di 250 dipendenti ma che effettuino trattamenti che presentano 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.

Qualora si realizzi una delle condizioni suindicate e una delle ipotesi indicate nel capitolo 1.1 che vede coinvolto il Delegato e che comportino l'inizio di una o più attività o uno o più servizi, quest'ultimo deve rivolgersi al D.P.O. aziendale o, in alternativa, all'Ufficio Privacy aziendale i quali lo supporteranno nella compilazione dei vari requisiti previsti dall'articolo 30 del GDPR.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

Si consiglia di seguire le seguenti indicazioni:

- Avere almeno un trattamento per ogni provvedimento a carattere generale dell'Autorità di Controllo (Garante) applicabile alla realtà di riferimento: a fronte di eventuali ispezioni sarà sicuramente apprezzata la produzione di almeno un trattamento per ciascun provvedimento a carattere generale. A titolo di esempio si riportano alcuni provvedimenti (per un elenco sempre aggiornato consultare la sezione "Provvedimenti e normativa" del sito istituzionale dell'Autorità Garante):
  - Autorizzazione generale al trattamento di dati sanitari
  - Linee guida su posta elettronica ed internet sul luogo di lavoro
  - Provvedimento Videosorveglianza
  - Linee guida in tema di pubblicazione per obblighi di trasparenza
  - Provvedimento sugli amministratori di sistema
  - Linee guida sul dossier sanitario
  - Linee guida sul fascicolo sanitario
  - Regolamento tipo per il trattamento dei dati sensibili e giudiziari per:
    - Regioni e Aziende Sanitarie ed altre agenzie regionali

Il Titolare deve, inoltre, tener conto che il Registro dei trattamenti deve avere le seguenti caratteristiche:

- **Completezza**: tutte le operazioni di trattamento dati personali per cui è applicabile il GDPR devono essere censite. Occorre indicare anche i trattamenti demandati a terze parti;
- **Aderenza alla realtà fattuale**: quanto descritto deve trovare una corrispondenza nella realtà fattuale, soprattutto nei documenti relativi ad altri aspetti privacy (informativa, accordi ex art. 28 con Responsabili, analisi dei rischi);
- **Legittimità**: Ciascun trattamento deve avere una sua base di liceità. Sarebbe opportuno parcellizzare il trattamento in funzione delle diverse basi di liceità: un trattamento dovrebbe avere una sola base di liceità per ogni finalità (vedi anche wp260);

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

- **Unitarietà**: Il Registro è dell'Ente/organizzazione nel suo complesso in capo al quale eventualmente sono posti obblighi giuridici e non alla singola struttura: per esempio un dipendente assegnato alla struttura XXX è dipendente dell'Ente, non di quella struttura;
- **Univocità degli interessati**: Non è vietato che un trattamento abbia più categorie di interessati, ma sarebbe opportuno individuare trattamenti con una o poche categorie di interessati. Infatti, può diventare problematico differenziare i diritti degli uni e degli altri, differenziare le diverse tipologie di dati trattati per ciascuna categoria e relazionare trattamenti con le informative, poiché quest'ultime dovrebbero rivolgersi a una categoria di interessati;
- **Periodo di conservazione**: Il periodo di conservazione è solitamente collegato alla normativa applicabile o ad altri obblighi contrattuali (soprattutto in un'ottica di minimizzazione). Si consiglia quindi di separare insiemi di operazioni che hanno scadenze temporali molto diverse. Per esempio l'evasione di un ordine dell'interessato ha una sua fine con la comprova della consegna del bene o servizio. Vi sono poi altri trattamenti (idealmente da separare) che riguardano gli adempimenti fiscali (che hanno durata tipicamente quinquennale) e altri trattamenti come la gestione del contenzioso civile che può derivarne (perdurano per 10 anni). In questi casi, in applicazione del principio di minimizzazione di cui all'art. 5 del GDPR) si consiglia, almeno in fase di affinamento del registro, di procedere inserendo i tre trattamenti di cui sopra (operativo specifico, fiscale generale per l'azienda, contenzioso civile generale per l'azienda);
- **Minimizzazione**: qualora un insieme di operazioni siano fatte da un sottoinsieme limitato di autorizzati e/o su un sottoinsieme dei dati si può valutare di identificare tale sottoinsieme come trattamento a sé stante. Considerazioni analoghe possono essere fatte per i supporti di trattamento.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

2.3.1.1. Compilare i campi del Registro dei trattamenti del "Titolare"

Per procedere con una corretta e completa compilazione del registro dei trattamenti in qualità di Titolare del trattamento, il Delegato, con il supporto del Team del DPO aziendale, deve procedere alla compilazione dei seguenti campi obbligatori ai sensi dell'art. 30 del GDPR :

1. **Finalità:** indicare la finalità o le varie finalità (lo scopo) per il quale viene eseguito il trattamento. Le finalità devono essere:
    - Determinate, il Titolare del trattamento deve definirle prima di iniziare il trattamento e non devono essere generiche, indefinite o illimitate;
    - Esplicite, il Titolare del trattamento deve comunicare le proprie finalità in maniera chiara e comprensibile a mezzo di informativa (Riferimento procedura "Stesura e gestione informative") che deve essere portata a conoscenza degli Interessati;
    - Legittime, il Titolare del trattamento deve stabilire delle finalità di trattamento che non siano *contra legem*.

    Ad ogni finalità del trattamento deve corrispondere almeno una **base giuridica** che renda lecito il trattamento stesso e che vari anche in relazione della tipologia di dati personali trattati:
    - Dati personali (art. 4 par. 1 punto 1): indicare una o più basi giuridiche (*lett. a) -f)*) contenute nell'art. 6, par. 1 del GDPR:
        - Qualora la base giuridica sia il consenso (lett. a)), verificare che sia stata consegnata l'informativa all'interessato in modo tale che il consenso sia informato e precisare le modalità di raccolta, la conservazione e la revoca del consenso
        - Qualora la base giuridica sia l'obbligo legale (*lett. c)*), indicare la norma di legge che obbliga il Titolare a trattare i dati personali;
        - Qualora la base giuridica sia l'Interesse Pubblico (*lett. e)*), indicare la disposizione normativa che individua tale Interesse ai sensi dell'art. 2 *ter* del D.Lgs. n. 196/2003 e s.m.i. e s.m.i.;
    - Categorie particolari di dati personali: indicare una o più basi giuridiche (*lett. a) -j)*) contenute nell'art. 9, par. 2 del GDPR:
        - Qualora la base giuridica sia il consenso (*lett. a)*, verificare che l'interessato abbia avuto accesso all'informativa, sia in forma

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

breve sia in forma estesa, in modo tale che il consenso sia informato e precisare le modalità di raccolta del consenso;

- Qualora la base giuridica sia l'Interesse Pubblico (*lett. g)*, indicare una delle ipotesi di Interesse Pubblico elencate nell'art. 2 *sexies* del D.Lgs. 196/2003 e s.m.i. e la relativa disposizione normativa che lo individua;
- Qualora la base giuridica sia l'Interesse Pubblico (*lett. g)*, indicare una delle ipotesi di Interesse Pubblico elencate nell'art. 2 *sexies* del D.Lgs. 196/2003 e s.m.i. e la relativa disposizione normativa che lo individua;

- Dati personali relativi a condanne penali e reati: indicare l'art. 10 del GDPR e le ipotesi elencate dall' art. 2 *octies* del D.Lgs. 196/2003 e s.m.i. con la relativa norma di legge o di regolamento (qualora previsto dalla legge) che autorizza il trattamento di tale tipologia di dati personali.

2. **Categoria di Interessati**: indicare la/le categoria/categorie di Interessati, cioè i soggetti a cui appartengono i dati personali oggetto del trattamento descritto (es. Dipendenti, Fornitori, pazienti, etc.) e precisare se in queste categorie sono presenti minori d'età o soggetti che presentano vulnerabilità particolari vulnerabilità (es. persone diversamente abili). La presenza di tali soggetti inciderà sul risultato dell'Analisi dei rischi e dell'eventuale DPIA;
3. **Tipologia dei dati personali**: indicare se si tratta di "dati personali comuni", specificando il dato personale trattato (es Nome, Cognome, Indirizzo, CF, etc.), se si tratta di "categorie particolari di dati personali", specificando nel dettaglio il dato trattato (es. dati biometrici, dati genetici, dati relativi allo stato di salute attuale e pregresso, convinzioni religiose o filosofiche, opinioni politiche, adesioni a partiti, sindacati, associazioni, etc.) o se si tratta di dati personali relativi a condanne penali e reati.

   In questa fase è necessario verificare che vi sia corrispondenza tra la tipologie di dati trattati e la/e base/i di liceità (illustrata precedentemente) indicata/e per ciascuna finalità.

   La presenza di "Categorie particolari di dati personali" e/o di "Dati relativi a reati e condanne penali" inciderà sul risultato dell'Analisi dei rischi e dell'eventuale DPIA.
4. **Destinatari**: indicare le categorie di destinatari a cui sono stati o saranno comunicati i dati personali, compresi quelli di paesi terzi od organizzazioni internazionali. Indicare, inoltre, la garanzia sul quale si basa il trasferimento ai sensi degli artt. 45,46, 47 e 49 del GDPR;

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

5. **Trasferimenti extra UE**: inserire, ove eseguiti, 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 par. 2 dell'articolo 49, la documentazione delle garanzie adeguate. La presenza di uno o più trasferimenti inciderà sul risultato dell'Analisi dei rischi e dell'eventuale DPIA;
6. **Periodo di conservazione**: indicare il periodo di conservazione dei dati personali trattati o, qualora non fosse possibile fornire un termine puntuale, indicare i criteri utilizzati per determinare il periodo di conservazione. I dati personali possono essere conservati sino al raggiungimento della finalità, oltre tale termine, qualora non vi siano delle specifiche previsioni normative, è possibile conservarli sino ai relativi termini di prescrizione (fiscale, civile, penale), secondo il massimario aziendale in uso;
7. **Supporti del trattamento/misure di sicurezza**: indicare i supporti utilizzati per eseguire le operazioni di trattamento, ad es. supporto cartaceo, server, applicazioni, PC, etc.

   Al fine di dare una corretta evidenza delle misure di sicurezza tecniche e organizzative di cui all'articolo 32 paragrafo 1, per ottemperare a quanto prescritto dall'art. 30, par. 1 *lett. g)* del GDPR, il Delegato deve coinvolgere i *Risk Owner* i quali dovranno fornire la propria valutazione sull'adeguatezza delle misure di sicurezza organizzative e tecniche applicate ai supporti col quale viene effettuato il trattamento e indicare eventuali e ulteriori misure da adottare per diminuirne il rischio .

Oltre alle informazioni suindicate, il Delegato può compilare, con il supporto del Team del DPO, il registro con ulteriori informazioni utili a gestire l'Accountability del Titolare/Responsabile del trattamento inserendo quanto segue:

1. **Numero scheda:** inserire l'allegato A o B e il numero della scheda di riferimento nel D.P.G.R. del 4 luglio 2016 n.9/R e relativo titolo (qualora il trattamento sia presente). In caso di nuovi trattamenti compilare il campo "codice trattamento" (es. Amministrazione personale 01)
2. **Denominazione del trattamento:** fornire una descrizione funzionale del processo di trattamento illustrando l'attività o il servizio in modo tale da circoscrivere il contesto nel quale viene eseguito il trattamento;
3. **Compilatore:** indicare colui che materialmente compila la scheda del Registro;
4. **Contitolare:** indicare se il trattamento avviene il regime di contitolarità;

5. **Denominazione sub trattamento:** qualora una attività presente nel D.P.G.R. non sia gestista totalmente dalla struttura, inserire il trattamento svolto dalla struttura
6. **Origine dei dati personali**: indicare la fonte di provenienza dei dati trattati. Tale informazione è utile per elaborare l'informativa corretta, più precisamente per redigere un'informativa *ex* art. 13 GDPR, qualora i dati siano stati raccolti presso l'Interessato, o per redigere un'informativa *ex* art 14 GDPR, qualora non siano stati raccolti *in toto* o parzialmente dall'Interessato (Riferimento procedura "Stesura e gestione informative");
7. **Operazioni e modalità di trattamento**: indicare le operazioni di trattamento che vengono effettuate tra quelle elencate nell'art. 4, par. 2 del GDPR. (manuale e/o automatizzata);
8. **"Organizzazione" del trattamento**: indicare la Struttura che all'interno dell'organizzazione del Titolare/Responsabile del trattamento effettua in maniera prevalente il trattamento in questione (che corrisponderà a quella di appartenenza del Delegato). Indicare le altre Strutture del Titolare del trattamento che collaborano al trattamento stesso, Titolari del trattamento (se il trattamento censito è eseguito in qualità di Responsabile del trattamento), eventuali fornitori con ruolo da Responsabili/Sub Responsabili del trattamento e/o Titolari autonomi;

Durante tutte le attività appena elencate, il Delegato ha la possibilità di chiedere consulenza al TEAM DEL DPO per chiarire eventuali dubbi relativi alla correttezza delle informazioni da inserire nel Registro dei trattamenti.

Se al termine del censimento il trattamento presenta le condizioni indicate nell'art. 35 del GDPR, nel WP 248 o nel Provvedimento generale del Garante dell'11 ottobre 2018, sarà necessario eseguire una DPIA prima di procedere concretamente al trattamento.

Inoltre, una volta compilato il registro dei trattamenti, per adempiere ai principi di trasparenza e legittimità del trattamento, e più in generale al principio di Accountability del Titolare, occorre verificare che per ogni trattamento corrisponda un'informativa ex artt. 13 o 14 del GDPR coerente (**N.B.** Una singola informativa può essere utilizzata per più trattamenti).

2.3.1.2. Compilare i campi del Registro dei trattamenti del "Responsabile"

Per procedere con una corretta e completa compilazione del registro dei trattamenti in qualità di Responsabile del trattamento, il Delegato deve procedere con la compilazione dei requisiti elencati nel paragrafo precedente con delle eccezioni, infatti vi sono delle informazioni che ai sensi dell'art. 30. par. 2 del GDPR non obbligatorio censire all'interno del Registro, ad esempio, le finalità del trattamento e la tipologia di dati personali trattati. Tuttavia, si tratta di elementi da prendere in considerazione per

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

eseguire l'analisi dei rischi e eventuali DPIA; quest'ultima è un onere del Titolare del trattamento che può chiedere supporto al Responsabile del trattamento il quale deve mettere a disposizione del Titolare tutte le informazioni utili a tal fine.

1.3.2. Inserire un nuovo trattamento di dati personali

Occorre procedere con l'inserimento di un nuovo trattamento qualora si verifichi una delle condizioni di attivazione di cui al punto 1.1.

Per procedere all'inserimento del trattamento all'interno del Registro dei trattamenti il Delegato coinvolge il team del DPO per il supporto alla compilazione dei campi di natura giuridica e il Risk owner per i campi di natura tecnico/organizzativa. Una volta compilate in maniera adeguata e esaustiva le sezioni del paragrafo 2.3.1.1. e sulla base delle indicazioni precisate nel paragrafo stesso, è possibile procedere ad una prima analisi dei rischi su:

- Gli elementi di natura tecnica/organizzativa (supporti utilizzati per eseguire il trattamento e il luogo fisico in cui vengono custoditi);
- Gli elementi di natura giuridica (Tipologia di dati personali, Categoria di Interessati e tipologia di operazioni come, ad esempio, larga scala, monitoraggio sistematico, geo localizzazione, etc.).

Una volta terminate le valutazione sopradescritte deve essere redatta un'informativa contenente tutte le informazioni richieste dagli artt. 13 o 14 del GDPR già presenti all'interno del registro.

2.3.3. Modificare il trattamento nei campi di natura giuridica

Occorre procedere con la modifica di un trattamento esistente qualora si verifichi una delle condizioni di attivazione di cui al punto 1.1.

La variazione può riguardare:

1. **La Finalità,** quando varia parzialmente o integralmente la finalità originaria per la quale i dati personali erano stati raccolti e trattati. Occorre, dunque, aggiornare l'informativa e renderla disponibile agli interessati affinché prendano visione delle modifiche del trattamento. Inoltre, è necessario rivalutare il periodo di conservazione in funzione della variazione della finalità;
2. **La Liceità,** come possibile conseguenza della variazione della finalità è possibile che sia necessario aggiornare anche la base giuridica che rende lecito il trattamento. Occorre, dunque, aggiornare l'informativa e renderla disponibile agli interessati affinché prendano visione delle modifiche del trattamento e,

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

qualora la base giuridica del nuovo trattamento sia il consenso, occorre raccogliere nuovamente o per la prima volta il consenso degli interessati;

3. **La Norma,** quando la liceità del trattamento deriva da un obbligo di legge o dall'esercizio di un pubblico interesse ed è modificata, integrata, promulgata o abrogata la norma di settore, occorre aggiornare il relativo campo;
4. **Gli Interessati,** quando variano (aumentano o diminuiscono) le categorie di interessati coinvolti nel trattamento. Nell'ipotesi in cui aumentino le categorie di interessati, occorre prestare attenzione all'eventuale presenza di persone fisiche vulnerabili (WP 248) minori d'età (se il trattamento è basato sul consenso, elaborare un'informativa semplificata affinché il consenso stesso non sia viziato dall'inosservanza dei principi di trasparenza e chiarezza, vedi WP 259 o all'aumento del numero degli interessati in relazione alla circoscrizione geografica (larga scala), parametri che possono modificare la valutazione sull'eventuale DPIA eseguita o incidere sull'esecuzione della stessa alla luce del nuovo trattamento;
5. **La tipologia di dati personali,** quando aumentano o diminuiscono le tipologie di dati personali trattati. Nell'ipotesi in cui aumentino, valutare che venga rispettato il principio ni minimizzazione e, qualora si tratti di "Categorie particolari di dati personali" o "Dati relativi a reati o condanne penali", controllare che sia stata inserita la relativa base giuridica che rende lecito il trattamento e che questi parametri influenzino la precedente valutazione sull'eventuale adozione o meno di una DPIA, soprattutto laddove sia già presente un parametro del WP 248;
6. **L'Origine,** quando i dati personali trattati vengono raccolti da una fonte distinta da quella prevista originariamente dal trattamento, occorre procedere con l'aggiornamento dell'informativa rendendola secondo il formato corretto prescritto dagli artt. 13 e 14 del GDPR;
7. **Destinatari,** quando i dati personali trattati vengono comunicati a categorie di destinatari differenti da quelli previsti originariamente dal trattamento (es. a seguito dell'introduzione di un nuovo obbligo normativo), occorre procedere con l'aggiornamento dell'informativa. Se i dati personali vengono traferiti extra UE deve essere indicata una delle misure di garanzia prescritte dagli artt. 45,46,47 e 49 del GDPR.

Terminata la modifica di uno o più dei campi sopracitati è necessario accertare che continuino a essere rispettati i principi degli artt. 5, 24, 32 del GDPR e se sia necessario procedere o meno con la DPIA.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

2.3.4. Modificare il trattamento nei campi di tecnici/gestionali

Occorre procedere con la modifica di un trattamento esistente qualora si verifichi una delle condizioni di attivazione di cui al punto 1.1

La variazione può riguardare:

1. **Uno o più Supporti,** quando viene ravvisato l'utilizzo di un ulteriore supporto o la dismissione di un supporto precedentemente utilizzato (es. utilizzo di un nuovo server, applicativo, client etc. o dismissione di un vecchio server, applicativo, client, etc.);
2. **Le misure di sicurezza dei supporti,** quando il Risk Owner ravvisa la necessità di aggiornare, introdurre nuove misure di sicurezza (es. aggiornamento SO, etc.) o dismettere supporti obsoleti (es. End of life di un server, etc.), anche a seguito di verifiche a seguito di *audit* del team del DPO;
3. **L'organizzazione interna,** quando vi sono delle variazioni che comportano l'introduzione/eliminazione di una struttura, modifiche del perimetro delle attività della stessa. In questi casi è necessario aggiornare le sezioni apposite del registro. Nelle ipotesi previste dai punti 1 e 2 del presente paragrafo occorre procedere con la verifica di quanto incide la variazione dei supporti sulla precedente Analisi dei rischi e sull'eventuale DPIA.

2.3.5. Storicizzare i trattamenti terminati

Occorre procedere con la "storicizzazione" dei trattamenti in essere ogni qualvolta in cui si verifica una delle condizioni di attivazione di cui al punto 1.1

L'archiviazione deve riguardare il Registro dei trattamenti in corso, infatti, è indispensabile tenere traccia di tutti i trattamenti eseguiti con i relativi riferimenti temporali (FAQ 8 ottobre 2018: "Istruzioni del Garante privacy sul registro dei trattamenti").

2.3.6. Audit del Registro dei trattamenti

Una volta censiti i trattamenti all'interno del Registro dei trattamenti, quest'ultimo deve essere sottoposto periodicamente ad attività di verifica/controllo. Infatti, trattandosi di uno strumento dinamico, i contenuti devono essere verificati e modificati ogni qualvolta si presenti una variazione nelle attività, servizi e processi del Titolare/Responsabile del trattamento. Tale attività deve essere svolta a mezzo di specifici soggetti designati, con la collaborazione del team del DPO.

Durante l'attività di audit, al fine di verificarne la correttezza dei contenuti, devono essere presenti i soggetti che hanno partecipato alla redazione dello stesso. La Direzione, con il supporto del team del DPO , verifica:

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

- La correttezza del ruolo col quale l'Ente/Azienda effettua il trattamento;
- Che la descrizione funzionale del trattamento sia completa ed esaustiva rispetto all'attività effettivamente svolta;
- Che sia stata indicata la finalità o le finalità del trattamento e che corrispondano a quelle effettivamente perseguite dall'Ente/Azienda (oltre che a essere esplicite, determinate e legittime);
- Che per ogni finalità indicata corrisponda una base giuridica che rende lecito il trattamento e che la base giuridica sia la più indicata per il trattamento di specie;
- Che le categorie di interessati identifichino correttamente le persone fisiche cui appartengano i dati personali oggetto di trattamento;
- Che le tipologie di dati trattati corrispondano effettivamente a quelle trattate durante l'attività di trattamento;
- Che le categorie di destinatari siano opportunamente indicate (es. soggetti ai quali devono essere comunicati i dati personali ai sensi di una precisa disposizione normativa) e che vi sia corrispondenza tra quelli censiti e quelli a cui vengono concretamente comunicati;
- Che a causa di una o più categorie di destinatari vi siano o meno dei trasferimenti extra UE. In tal caso è necessario indicare la garanzia con la quale avviene il trasferimento (artt. 45,46,47 e 49);
- Che sia rispettato il periodo di conservazione o i criteri per determinarlo e che quanto censito corrisponda effettivamente a quanto eseguito;
- Che i supporti censiti corrispondano a quelli utilizzati per eseguire il trattamento. Inoltre è necessario verificare l'adeguatezza dei supporti, in particolar modo quelli di natura informatica, verificandone l'obsolescenza, che le misure di sicurezza applicate siano adeguate allo stato dell'arte e che venga rispettato il principio di minimizzazione evitando l'utilizzo sproporzionato degli stessi.

Se censite, il Titolare per mezzo del Gruppo Privacy verifica anche:

- Che l'origine dei dati personali corrisponda a quella effettiva;
- Che le operazioni del trattamento corrispondano a quelle censite;
- Che la componente gestionale/organizzativa del trattamento sia aggiornata, cioè che i componenti della struttura siano aggiornati e appositamente autorizzati (Persone autorizzate e ADS) e che siano precisati eventuali Responsabili/Sub Responsabili del trattamento.

Al termine dell'attività di *audit*, se vengono modificate parte delle informazioni censite, occorre valutare quanto la variazione incide sull'analisi dei rischi e sull'eventuale DPIA eseguita.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

2.3.7. Revisione della procedura

A seguito di eventuali discordanze tra quanto censito e quanto accertato durante gli *audit* e attività di verifica, di profondi mutamenti del contesto organizzativo, si possono prevedere periodiche revisioni. Tale revisione è comunque obbligatoria ogni 5 anni.

Sede legale: Via Po, 11 - 10034 CHIVASSO (TO)
Tel. +39 011.9176666
Sede amministrativa: Via Aldisio, 2 - 10015 IVREA (TO)
Tel. +39 0125.4141
www.aslto4.piemonte.it
P.I./Cod. Fisc. 09736160012

2. RUOLI E RESPONSABILITÀ

Ruoli _____ Passi della Procedura	*Delegato*	*Risk Owner*	TEAM del DPO	Ufficio Privacy
1. Attivazione	R	===	C	C
1. Nuovo trattamento	R	C	C	C
2. Modificare trattamento nei campi di natura giuridica	R	===	C	C
3. Modificare trattamento nei campi di natura gestionale/informatica	C	R	C	I
4. Storicizzare trattamenti terminati	R	C	C	C
5. Audit registro	C	C	R	C
6. Revisione della procedura	===	===	C	R

Figura n. 1

Legenda: R = è Responsabile
C = Collabora
I = Informato

Indicare con R l'unico ruolo responsabile del passo procedurale e con C il/i ruolo/i che collaborano con il responsabile.

Indicare e/o descrivere eventuali tecniche e strumenti di supporto utilizzati per l'esecuzione della procedura (ad es. check-list, programmi di utilità, ecc.).

In caso non ce ne siano, scrivere:

Non sono previste ed utilizzate tecniche e strumenti particolari per l'esecuzione di questa procedura.