PROVINCIA DI CUNEO

REGOLAMENTO PROVINCIALE

PER L'ATTUAZIONE DEL

REGOLAMENTO EUROPEO N.679/2016

SULLA PROTEZIONE DEI DATI PERSONALI

APPROVATO CON D.C.P. no. 16 del 8.4.2019

Sommario

1. Principali novità introdotte dal Regolamento Europeo (GDPR) N. 679/2016

Il GDPR ha segnato una linea di demarcazione tra le precedenti discipline in materia di protezione dei dati personali partendo da due ambiti significativi:

- responsabilizzazione, o *accountability*, e le sue varie componenti;
- diritti degli interessati.

2. Approccio basato sulla responsabilizzazione

Il sistema della "responsabilizzazione" rappresenta l'elemento fondamentale per garantire in modo evidente e certo la conformità al GDPR che affida al Titolare e al Responsabile l'adozione di adeguate misure di sicurezza.

Nell'ambito del GDPR il principio di *accountability* può tradursi come responsabilità da comprovare tramite evidenze atte a dimostrare le valutazioni, le scelte e le misure adottate a garanzia della protezione dei dati personali.

3. Individuazione dei ruoli e divisione dei compiti

Il GDPR presuppone quindi la definizione di un modello organizzativo che preveda ruoli, compiti e responsabilità in capo ai vari attori coinvolti nelle attività di trattamento dei dati personali.

Con tale prospettiva assegna al Titolare, anche in collaborazione con il Responsabile (uno o più), il compito di valutare preventivamente e autonomamente le modalità, le garanzie, i limiti dei trattamenti e l'impatto dei trattamenti sulla protezione dei dati.

Il Titolare del trattamento e il Responsabile rappresentano i ruoli chiave per l'applicazione delle disposizioni del GDPR a cui sono in via generale riconducibili le relative responsabilità.

3.1 Titolare del trattamento dei dati personali

La definizione di Titolare del trattamento nel GDPR identifica, tra i soggetti che possono ricoprire il ruolo, l'autorità pubblica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

La Provincia di Cuneo agisce quindi nella veste di Titolare del trattamento attraverso gli organi e i soggetti preposti in relazione alle regole dell'ordinamento giuridico.

3.2 Responsabile del trattamento dei dati personali

Secondo la *ratio* del GDPR, quando si fa riferimento al Responsabile del trattamento deve intendersi soltanto il Responsabile esterno che agisce per conto del Titolare dietro affidamento di prestazioni o servizi.

Viene confermato il potere del Titolare di definire il proprio assetto organizzativo ed attribuire a soggetti interni all'organizzazione funzioni specifiche e compiti a presidio del sistema di gestione della protezione dei dati personali.

3.3 Organizzazione della Provincia di Cuneo

Il vigente "Regolamento di organizzazione degli uffici e dei servizi" definisce la struttura organizzativa della Provincia di Cuneo, disciplinandone i criteri e le modalità di organizzazione degli uffici e dei servizi.

3.3.1. Responsabile della Protezione dei dati - Data Protection Officer (DPO)

Il Responsabile della protezione dei dati - DPO della Provincia di Cuneo può essere sia un soggetto esterno, che un dipendente dell'Ente, in possesso di comprovata e rilevante professionalità ed elevata conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché in grado di assolvere ai compiti allo stesso attribuiti dalla vigente normativa in materia.

Nel caso in cui sia un dipendente dell'Ente, il DPO è scelto tra il personale a tempo indeterminato inquadrato nella categoria professionale "D" del contratto collettivo del comparto del personale non dirigente oppure tra il personale con qualifica dirigenziale.

Al Responsabile della protezione dei dati - DPO competono funzioni e poteri previsti dalla normativa vigente in materia, che il medesimo svolge ed esercita in totale autonomia ed in posizione di indipendenza, rispondendo direttamente al vertice dell'Amministrazione, quale Titolare del trattamento dei dati personali.

Il DPO esercita, in particolare, funzioni di:

1) informazione e consulenza al Titolare e al Responsabile, nonché ai dipendenti che eseguono i trattamenti, in ordine agli obblighi derivanti dal Regolamento UE o da altre disposizioni dell'Unione o degli stati membri;
2) sorveglianza sull'osservanza del Regolamento UE e di altre disposizioni dell'Unione e degli Stati relative alla protezione dei dati;
3) sorveglianza sull'osservanza delle politiche di protezione dei dati del Titolare o del Responsabile, anche con riguardo alla distribuzione dei compiti e delle responsabilità, nonché alla formazione delle persone che trattano i dati e alle relative attività di controllo;
4) formulazione del parere, se richiesto, sulla valutazione di impatto e sorveglianza dello svolgimento;
5) cooperazione con l'Autorità di controllo e punto di contatto con essa;
6) considerazione dei rischi relativi ai trattamenti tenendo conto dell'ambito di applicazione, del contesto e delle finalità.

Nell'ambito delle funzioni di cui al punto 1), il DPO fornisce, in particolare, consulenza ai dirigenti in ordine alla conformità delle attività di trattamento svolte rispetto alle norme in materia, al fine di individuare soluzioni idonee a bilanciare le esigenze organizzativo-gestionale dell'Ente con la protezione dei dati personali.

Nello svolgimento dei compiti e delle funzioni attribuite, al DPO verrà assicurata l'autonomia nello svolgimento dei compiti e non verranno fornite istruzioni per l'esercizio delle sue funzioni, in applicazione dell'art. 38 punto 3 del GDPR.

Fermo restando le funzioni descritte negli artt. da 37 a 39 del GDPR, i compiti specifici affidati al DPO sono dettagliati nel relativo atto di nomina, ovvero in specifici atti successivi.

La nomina del DPO è disposta con provvedimento del Presidente della Provincia.

3.3.2. Personale dirigente

Il GDPR definisce caratteristiche soggettive e responsabilità del Titolare trattamento dei dati personali. Pur non prevedendo espressamente la figura dell'incaricato al trattamento dei dati, il GDPR non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (art. 4, n. 10 del GDPR).

Sulla base del vigente assetto organizzativo dell'Ente, al personale dirigente è quindi rimesso il presidio in tema di protezione dei dati personali, in coerenza con la previsione dell'art. 107 del D. Lgs. n. 267/2000 e dell'art. 14 del vigente Regolamento di organizzazione degli uffici e dei servizi.

Nell'ambito del quadro generale in materia di protezione dei dati, i dirigenti sono designati dal Titolare con specifici compiti e funzioni connesse al trattamento dei dati ed in particolare:

a) censire, gestire ed aggiornare i trattamenti dei dati personali nell'apposito registro (punto 5), con esclusivo riguardo agli ambiti di pertinenza della struttura di riferimento, assicurando la coerenza e la compatibilità tra gli scopi perseguiti e le attività di trattamento effettuate, a tutela della riservatezza, correttezza ed integrità dei dati;
b) adottare misure organizzativo-gestionali adeguate a garantire la protezione dei dati personali, in relazione e nei limiti delle competenze relative alla posizione ricoperta;
c) individuare ed autorizzare il personale della Provincia di Cuneo a trattare i dati personali, con riguardo alle risorse e alle funzioni facenti capo alla struttura organizzativa gestita;
d) individuare, in ogni settore, il personale preposto all'attuazione degli adempimenti previsti dalla normativa sulla privacy (c.d. "referenti privacy") ed in particolare alla predisposizione e messa disposizione degli interessati delle informative, alla gestione del registro dei trattamenti di dati personali e del registro dei *data breach*;
e) predisporre gli atti di nomina del Titolare relativi ai Responsabili del trattamento dei dati personali, che operano per conto della Provincia per l'esecuzione di attività inerenti gli ambiti e le strutture organizzative di competenza;
f) vigilare sull'attività svolta dalle persone autorizzate a trattare i dati e da ogni altro soggetto che collabora con la struttura di competenza e/o agisce per conto del Titolare del trattamento;
g) fornire agli interessati le informative ex artt. 13 e 14 del GDPR ed assicurare agli stessi l'esercizio dei diritti previsti agli artt. da 15 a 22 del GDPR, provvedendo alle relative comunicazioni;
h) fornire al DPO la necessaria collaborazione nell'esercizio dei suoi compiti e riferire al medesimo eventuali casi di violazione dei dati personali (*data breach*);
i) coinvolgere il DPO nelle questioni riguardanti la protezione dei dati per le conseguenti valutazioni.

In merito allo svolgimento dei compiti elencati, il personale dirigente può consultare il DPO.

3.3.3. Persone autorizzate

Il GDPR prevede che le operazioni di trattamento possono essere effettuate solo da persone autorizzate che operano sotto la diretta autorità del Titolare o del Responsabile.

In via generale, i dipendenti dell'Amministrazione, in relazione allo specifico ambito lavorativo coordinato e gestito, trattano dati personali e, in quanto tali, devono essere autorizzati al trattamento dal Titolare o dai rispettivi dirigenti (punto 3.3.2. lettera c)).

3.3.4. Compiti e responsabilità del settore Sistemi Informativi

Nell'ambito dell'organizzazione della Provincia di Cuneo assume particolare rilievo, per il sistema di *data protection*, il ruolo del settore Sistemi Informativi, tenuto conto che i trattamenti e la gestione dei dati, in un contesto particolarmente digitalizzato, avvengono prevalentemente con modalità informatizzate. Deve essere pertanto assicurato un livello di protezione dei dati personali correlato alla rapidità dell'evoluzione tecnologica e alla necessità di reagire tempestivamente con misure adeguate a tali processi innovativi.

In considerazione di ciò e sulla scorta del vigente assetto organizzativo dell'Ente, al settore Sistemi Informativi sono demandate le funzioni, le attività e le responsabilità connesse ai profili tecnico-informatici, con particolare riguardo alla gestione della sicurezza dei sistemi informativi, degli applicativi e delle reti di telecomunicazioni.

Il settore Sistemi Informativi è tenuto, nei limiti delle risorse economiche e del personale messo a disposizione dall'Ente, a mettere in atto misure tecniche ed organizzative per garantire la sicurezza informatica nei termini previsti dalle norme in materia, predisponendo, nel rispetto del principio di *accountability*, evidenze documentali circa le azioni intraprese, le attività svolte e le caratteristiche dei sistemi.

Nell'ambito delle funzioni ascritte al settore Sistemi Informativi rientrano anche il presidio e la gestione degli amministratori di sistema.

Il settore Sistemi Informativi si raccorda con il settore Personale, qualora le misure adottate, anche in relazione all'uso di nuove tecnologie, abbiano riflessi sul rapporto di lavoro del personale e/o di natura sindacale.

3.4 Responsabili del trattamento

Il GDPR definisce con puntualità gli strumenti per nominare i Responsabili del trattamento.

Prevede, infatti, che a vincolare il Responsabile al Titolare sia un contratto (o altro atto giuridico conforme al diritto nazionale) che disciplini i rapporti tra le parti e che individui la natura, la finalità del trattamento, la durata, la categoria di dati da trattare e di interessati, ecc.

La nomina del Responsabile esterno, affidatario di un servizio o di una prestazione, va pertanto definita attraverso accordo contrattuale o con un atto equivalente contenente le istruzioni, le responsabilità e gli obblighi da rispettare, ivi compreso l'adozione delle misure di sicurezza, la tenuta del registro dei trattamenti, la nomina del DPO nei casi previsti dal GDPR.

3.4.1 Sub Responsabili de/ trattamento

Il GDPR permette ai Responsabili del trattamento di nominare sub-responsabili, purché autorizzati preventivamente dal Titolare. In tal caso il Responsabile vincola il sub-responsabile con un contratto (o altro atto giuridico conforme al diritto nazionale) che contenga gli stessi obblighi previsti nel contratto stipulato tra il primo responsabile e il Titolare. Il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità degli adempimenti degli obblighi dell'altro responsabile.

4. Misure di sicurezza

Il GDPR ha introdotto la nozione di "misure adeguate" ed assegna al Titolare del trattamento e al Responsabile del trattamento il compito di individuare le misure tecniche ed organizzative più adeguate in relazione alla tipologia dei trattamenti e ai rischi che incombono sui dati.

Le misure di sicurezza devono essere individuate sulla base di un'attenta valutazione dei rischi "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche il rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*" (art. 32 punto 1 GDPR).

4.1. Valutazione dei rischi

Richiamato il punto 3.3.4., il settore Sistemi Informativi aggiorna le misure di sicurezza, valutando i rischi collegati alle operazioni di trattamento che incombono sui dati personali in formato digitale ed i conseguenti potenziali effetti, allo scopo di mettere in atto le contromisure idonee a prevenire le relative minacce.

Richiamato il punto 3.3.2., ogni settore adotta opportune misure organizzativo-gestionali adeguate a garantire la protezione dei dati personali trattati, inclusi i dati in formato cartaceo.

4.2 Valutazione di impatto

Il GDPR introduce l'obbligo di valutare i rischi che possono generare un impatto negativo sulla libertà e i diritti degli interessati. La valutazione di impatto o D.P.I.A. (*Data Protection Impact Assessment*) va condotta preventivamente quando un tipo di trattamento, allorché prevede l'uso di particolari tecnologie, considerati la natura, il contesto e l'oggetto può presentare un rischio elevato per i diritti e le libertà delle persone.

In seguito alla valutazione di impatto, il Titolare può assumere autonomamente la decisione di iniziare il trattamento previa adozione delle necessarie misure per ridurre o mitigare i rischi, interpellando l'Autorità Garante solo se dopo l'adozione delle misure permangono rischi residuali elevati.

Il compito di effettuare la D.P.I.A. sui trattamenti è rimesso al settore interessato, con il supporto del settore Sistemi Informativi per tutti gli aspetti tecnico-informatici, e in tale ambito va consultato il DPO, che rilascia il parere se richiesto.

4.3 Data Breach

Il GDPR (artt. 33 e 34) ha introdotto per tutti i Titolari del trattamento l'obbligo di notificare all'Autorità di controllo, entro 72 ore dalla conoscenza dell'evento, i casi di violazione dei dati personali e di comunicare agli interessati l'accaduto quando ricorrono particolari situazioni (rischio elevato per i diritti e le libertà delle persone).

La notifica al Garante non è sempre obbligatoria, ma è dovuta quando la probabilità del rischio di compromettere i diritti degli interessati è elevata. L'esonero della comunicazione, oltre che in tali casi, vale anche nei confronti degli interessati quando il Titolare del trattamento ha messo in atto misure di sicurezza adeguate come, ad esempio, quelle destinate a rendere i dati incomprensibili (crittografia).

Il settore interessato da *data breach* su dati personali digitali, con il supporto degli amministratori di sistema del settore Sistemi Informativi, informa tempestivamente il DPO ed il Titolare, per la valutazione congiunta del fenomeno e per le eventuali comunicazioni al Garante e agli interessati.

Analogamente, il settore interessato da *data breach* su dati personali in formato cartaceo, informa tempestivamente il DPO ed il Titolare, per la valutazione congiunta del fenomeno e per le eventuali comunicazioni al Garante e agli interessati.

Compete al settore Sistemi Informativi definire o consolidare le procedure per reagire ai fenomeni classificabili come *data breach* sui dati personali digitali e gestire l'emergenza. Il personale del settore interessato dalla violazione, con il supporto degli amministratori di sistema del settore Sistemi Informativi, registra nell'apposito registro gli attacchi informatici subiti che abbiano determinato violazioni di dati personali.

Compete ad ogni settore definire o consolidare le procedure per reagire ai fenomeni classificabili come *data breach* sui dati personali su supporti cartacei, gestire l'emergenza e registrare nell'apposito registro la violazione subita.

4.4 Principio di privacy by design by default

Il principio di *privacy by design e by default* introduce una formula innovativa per la gestione dei dati personali in base al quale gli strumenti e le modalità impiegati per il trattamento dei dati vanno progettati già all'origine (*by design*) in modo tale che siano garantite per impostazione predefinita (*by default*) la tutela della riservatezza e la protezione dei dati personali.

In questo senso, laddove i mezzi e i servizi sono offerti da terzi, già in sede di predisposizione dei documenti tecnico - amministrativi connessi all'espletamento delle procedure ad evidenza pubblica, è necessario che i settori prevedano i criteri per rispettare tale principio ovvero la protezione dei dati per impostazione predefinita.

5. Registro delle attività di trattamento

L'art. 30 del GDPR prevede che il Titolare e il Responsabile tengano un registro delle attività del trattamento contenente una serie di informazioni.

Il registro rappresenta l'elemento centrale per la *governance* del modello di gestione privacy e va tenuto in forma scritta, anche in formato elettronico.

Nell'ambito della Provincia di Cuneo, la tenuta del registro in formato elettronico, unico per tutto l'ente, è affidata al DPO, il quale nell'esercizio delle proprie funzioni coordina le attività di aggiornamento sistematico dei dati del registro che i singoli settori devono svolgere sistematicamente (punto 3.3.2 lettera a)) .

6. Monitoraggio

Il modello di gestione della privacy illustrato è sottoposto a costante monitoraggio da parte dell'Amministrazione, allo scopo di intervenire rapidamente, anche su proposta del DPO, sull'assetto organizzativo in caso di modifiche normative o dell'evoluzione tecnologica o dell'introduzione di nuove politiche di gestione dei dati personali.