UNIONE DEI COMUNI
DEL CIRIACESE E BASSO CANAVESE

REGOLAMENTO UNIONALE PRIVACY

Approvato con deliberazione del Consiglio dell'Unione n. 13 del 10.05.2023

(Testo in vigore dal 10.05.2023)

INDICE

Art. 1 Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento Generale Protezione Dati di seguito indicato con "GDPR" e della normativa interna, in relazione alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, da parte dell'Unione dei Comuni del Ciriacese e del Basso Canavese.

Art. 2 Titolare del trattamento

1. L'Unione dei Comuni del Ciriacese e del Basso Canavese (di seguito indicato con "Titolare" o "Unione"), rappresentata ai fini previsti dal GDPR dal Presidente *pro tempore*, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee.
Il Presidente può delegare le relative funzioni al personale dell'Unione, nominato secondo quanto previsto dall'art. 4 del presente atto e ai sensi dell'art. 2 *quaterdecies* del Codice Privacy.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate in concreto a garantire la conformità del trattamento ai dettami del GDPR.
Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

4. Il Titolare garantisce l'adozione di misure idonee a fornire all'interessato:
a) le informazioni indicate dall'art. 13 del GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
b) le informazioni indicate dall'art. 14 del GDPR, qualora i dati personali non siano ottenuti presso lo stesso interessato.

5. Fermo restando quanto disciplinato all'art. 9 del presente Regolamento, nel caso in cui un tipo di

trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare s'impegna ad effettuare una valutazione di impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 del GDPR.
A tal fine, il Titolare è tenuto a considerare l'impiego di nuove tecnologie, la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.
Per la valutazione dei tipi di trattamento da sottoporre a Valutazione d'Impatto, l'Unione deve tener conto altresì del Provvedimento del Garante Privacy n. 467 dell'11 ottobre 2018, in cui sono elencate a titolo esemplificativo ma non esaustivo le tipologie di trattamenti da sottoporre a valutazione d'impatto.

6. Il Titolare, inoltre, provvede a:

a) nominare i dipendenti dell'amministrazione quali "soggetti autorizzati al trattamento" ai sensi dell'art. 2-*quaterdecies* del Codice Privacy e dell'art. 29 GDPR;

b) nominare, tra i soggetti indicati al punto *a*), uno o più "Referenti Interni" individuati nel Direttore e/o nei Dirigenti dei singoli settori in cui si articola l'organizzazione e che possono essere preposti al trattamento dei dati presenti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;

c) nominare il "Responsabile della Protezione dei Dati" (DPO/DPO);

d) nominare quali "Responsabili esterni del trattamento" i soggetti terzi/esterni pubblici o privati affidatari di attività e servizi per conto dell'Unione ai sensi dell'art. 28 GDPR.
Ciò anche relativamente alle banche dati gestite da soggetti esterni all'Ente in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge per la realizzazione di attività connesse alle attività istituzionali;

e) predisporre gli elenchi dei Responsabili esterni del trattamento e dei soggetti autorizzati al trattamento di cui ai precedenti punti a) e d).

7. In caso di esercizio associato di funzioni e servizi, allorché due o più Titolari determinino congiuntamente e mediante accordo le finalità ed i mezzi del trattamento, il Titolare valuta la necessità di concludere un accordo di contitolarità secondo quanto disciplinato dall'art. 26 del GDPR.
Tale accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile. L'accordo può individuare un punto di contatto comune per gli interessati.

8. L'Unione favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 3 Liceità e finalità del trattamento

1. I trattamenti effettuati dall'Unione sono leciti se ricorre una delle seguenti condizioni:
a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per l'esercizio delle funzioni amministrative che riguardano la popolazione, l'ambiente e il territorio, affidate all'Unione in base alla vigente legislazione. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
In questo caso il titolare deve attenersi a quanto disposto dall' art. 2-*ter* del Codice Privacy.
b) l'adempimento di un obbligo legale al quale è soggetto il Unione. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
c) l'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 4 Autorizzati al trattamento

1. I dipendenti dell'Unione devono essere designati quali "soggetti autorizzati al trattamento", mediante apposito atto sottoscritto dal Presidente.
L'atto di designazione deve tassativamente indicare:
a) la natura e la tipologia dei trattamenti assegnati;
b) il tipo di dati personali oggetto di trattamento e le categorie di interessati;
c) il nome della/e banca/banche dati su cui il soggetto autorizzato al trattamento opera;
d) le istruzioni da seguire nelle operazioni di trattamento.

2. I Dirigenti di Settore, le Posizioni Organizzative ed il Segretario, già nominati quali "soggetti autorizzati al trattamento" secondo quanto previsto al punto 1 di questo articolo, possono essere nominati altresì "Referenti Interni".
Tale ruolo comporta la gestione delle banche dati personali esistenti nell'articolazione organizzativa di competenza. Il Referente Interno deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

Art. 5 Responsabili esterni del trattamento

1. Per il trattamento di dati, anche appartenenti alle categorie di dati particolari di cui all'art. 9 del GDPR, il Titolare può avvalersi di soggetti pubblici o privati che forniscano adeguate garanzie in termini di conoscenza specialistica, capacità ed affidabilità.
Tali soggetti, svolgendo il trattamento per conto del Titolare, devono essere nominati quali "Responsabili Esterni del Trattamento" mediante un contratto o altro atto giuridico e devono garantire la costante adozione di misure tecniche e organizzative volte a garantire che i trattamenti siano effettuati in conformità al GDPR.

2. I contratti o gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, par. 3, del GDPR, potendo basarsi altresì su clausole contrattuali tipo adottate dalla Commissione europea.
In ogni caso, tali atti devono indicare:

a) le finalità perseguite
b) la tipologia dei dati
c) la durata del trattamento
d) gli obblighi del Responsabile del trattamento
e) le modalità di trattamento
f) le modalità di restituzione all'Ente o di cancellazione dei dati al termine del contratto.

3. Il Titolare può autorizzare il Responsabile esterno di cui al punto 1 del presente articolo (cd. primario) a nominare ulteriori sub-responsabili del trattamento relativamente a specifiche attività, purché ciò avvenga nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario.
Le operazioni di trattamento possono essere effettuate esclusivamente da soggetti appositamente incaricati dal Responsabile primario o comunque operanti sotto la sua diretta autorità.
I soggetti sub-responsabili devono attenersi alle istruzioni loro impartite per iscritto dal Responsabile primario ed agire esclusivamente nell'ambito dei trattamenti autorizzati da quest'ultimo.
Il Responsabile primario risponde anche dinanzi al Titolare dell'operato del/i sub-responsabile/i, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del/i sub-responsabile/i.

4. Il Responsabile esterno del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso ai dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

5. Il Responsabile esterno del trattamento dei dati provvede, per il proprio ambito di competenza,

a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

a) alla tenuta di un autonomo e distinto Registro delle categorie di attività di trattamento svolte per conto del Titolare;
b) all'adozione di idonee misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti;
c) alla sensibilizzazione e alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
d) alla designazione del Responsabile per la Protezione dei Dati (DPO), se previsto per legge;
e) ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
f) ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso in cui il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art. 6 Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "DPO" o "RPD") è designato tra i dipendenti di ruolo dell'Unione ovvero tra professionisti esterni, nel rispetto di quanto stabilito dal Garante per la Protezione dei Dati Personali nel Documento di indirizzo su designazione, posizione e compiti del Responsabile della Protezione dei Dati in ambito pubblico, allegato al Provvedimento del 29 aprile 2021.
Il DPO può essere scelto fra i dipendenti del Unione, purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione dell'Unione.
Il Titolare provvede affinché il DPO mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.
Nel caso in cui il DPO non sia un dipendente dell'Ente, l'incaricato persona fisica è selezionato fra soggetti aventi le medesime qualità professionali richieste al dipendente, che abbiano maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili.

2. I compiti attribuiti al DPO sono indicati in apposito contratto di servizi.
In particolare, il DPO è incaricato dei seguenti compiti:

a) informare ed assistere il Titolare e gli autorizzati in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati.

In tal senso il DPO può indicare al Titolare e/o ai Referenti Interni i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, ed a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento.

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;

d) fornire se richiesto un parere in merito alla necessità di effettuare una valutazione di impatto sulla protezione dei dati (DPIA). In caso di parere positivo, l'DPO vigila sulla metodologia utilizzata dal Titolare nel condurre la DPIA, sulle misure tecniche ed organizzative adottate e sulle conclusioni raggiunte.
Il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Tuttavia, nel caso in cui la decisione assunta determini condotte difformi da quelle raccomandate dal DPO, il Titolare è tenuto a motivare specificamente tale decisione.

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del DPO è comunicato dal Titolare al Garante;

3. Il Titolare del trattamento assicura che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, con specifico riferimento ad eventuali violazioni di dati (cd. *Data Breach).*

4. Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle capacità di bilancio dell'Ente.
In particolare è assicurato al DPO:

a) supporto attivo per lo svolgimento dei compiti da parte del Presidente, del Direttore Generale e dei Dirigenti, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;

b) tempo sufficiente per l'espletamento dei compiti ad esso affidati;

c) supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno personale; se necessario l'Ente deve provvedere alla costituzione di un ufficio o di un gruppo di lavoro (formato dal DPO stesso e dal rispettivo personale);

d) comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;

e) accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

5. La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento; in

particolare, risultano con la stessa incompatibili:
a) il Responsabile per la prevenzione della corruzione e per la trasparenza;
b) il Referente Interno del trattamento;
c) qualunque incarico o funzione che comporti la determinazione di finalità o mezzi del trattamento.

6. Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare egli non deve ricevere istruzioni in merito al loro svolgimento, né sull'interpretazione da dare ad una specifica questione attinente alla normativa in materia di protezione dei dati.
Il DPO non può essere rimosso o penalizzato dal Titolare del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare.
Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il GDPR o con le indicazioni da lui fornite, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare del trattamento.
Per garantire l'indipendenza del DPO, il Titolare vigila affinché non si configurino in capo al RDP eventuali conflitti di interessi.

7. Il Titolare garantisce la pubblicazione ed il costante aggiornamento dei dati di contatto del DPO sul sito web istituzionale dell'Amministrazione.

Art. 7 Sicurezza del trattamento

1. Il Titolare del trattamento mette in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure organizzative di sicurezza minime:
a) nomina per iscritto del personale autorizzato
b) istruzioni per il trattamento
c) accesso controllato
d) armadi chiusi
e) procedura modifica credenziali

f) codici di condotta/policy unionali
g) formazione
h) nomina per iscritto responsabili esterni

4. Costituiscono misure tecniche di sicurezza minime:
a) autenticazione
b) autorizzazione
c) cifratura dei dati
d) separazione dei dati
e) firewall
f) antivirus

5. La conformità del trattamento dei dati al GDPR in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

6. Il Titolare si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure ai soggetti autorizzati al trattamento e a chiunque agisca per suo conto ed abbia accesso a dati personali.

7. Il trattamento di categorie particolari di dati (art. 9 GDPR) avviene rispettando le disposizioni di cui agli artt. 2 *sexies* e 2 *septies* del Codice Privacy e 9 GDPR.

Art. 8 Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento contiene le seguenti informazioni:
a) il nome ed i dati di contatto del Unione, del Presidente e/o del Referente Interno, eventualmente del Contitolare del trattamento e del DPO;
b) l'indicazione delle diverse macro aree di attività svolte dall'Ente;
c) una breve descrizione delle attività di trattamento;
d) le finalità del trattamento;
e) le basi giuridiche sulle quali si fonda il trattamento di dati;
f) le principali operazioni di trattamento effettuate: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione e ogni altra operazione applicata a dati personali;
g) l'indicazione delle categorie di dati personali;
h) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
i) la sintetica descrizione delle categorie di interessati;
l) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
m) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione

internazionale;
n) il nome ed i dati di contatto di eventuali Responsabili del trattamento;
o) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 7.

2. Il Registro è tenuto dal Titolare presso gli uffici della struttura organizzativa dell'Unione in forma telematica e/o cartacea; nello stesso possono essere inserite ulteriori informazioni.

3. Ove lo ritenga opportuno, l'Unione può provvedere a redigere - oltre al Registro delle attività di trattamento di cui al punto 1 del presente articolo – ulteriori registri con le attività di trattamento dei singoli Servizi/Direzioni.

Art. 9 Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, in particolare se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve effettuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. Tale procedura è rivolta essenzialmente a determinare l'origine, la natura e la gravità dei rischi dei trattamenti posti in essere dal titolare, i quali potrebbero creare un danno agli interessati.

2. Ai fini della decisione di effettuare o meno la DPIA, si tiene conto dell'Elenco delle tipologie di trattamento soggette o non soggette a valutazione d'impatto del Provvedimento del Garante Privacy n. 467 dell'11 ottobre 2018 nonché dei Provvedimenti futuri adottati ai sensi dell'art. 35, par. 4-6, del GDPR.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche.
Fermo restando quanto indicato dall'art. 35, par. 3, del GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

accessibile al pubblico;

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 GDPR;
e) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi uno o più criteri sopra indicati, occorre in via generale condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Unione.
Il Titolare deve consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO monitora lo svolgimento della DPIA.
Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.
Il Referente Interno, il responsabile della sicurezza dei sistemi informativi- se nominato -, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. Il DPO può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento. Il Referente Interno, il responsabile della sicurezza dei sistemi informativi- se nominato-, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA deve contenere:

a) una descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali

(hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) la valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo di conservazione;
- delle informazioni fornite agli interessati;
- dei diritti degli interessati;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati.

c) la valutazione dei rischi per i diritti e le libertà degli interessati, valutando la probabilità e gravità dei rischi rilevati.

d) l'individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR.

7. Il Titolare può raccogliere le opinioni degli interessati e/o dei loro rappresentanti.

8. Il Titolare prima di procedere al trattamento, se il risultato della DPIA indica l'esistenza di un rischio residuo elevato, deve consultare il Garante Privacy ai sensi dell'art. 36.

9. La DPIA deve essere effettuata, con eventuale riesame delle valutazioni condotte, anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

10. L'Ente può pubblicare in apposita sezione del sito istituzionale una sintesi delle principali risultanze della valutazione d'impatto ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Art. 10 Violazione dei dati personali

1. Per violazione dei dati personali (di seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati del Unione.

2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica

dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. A tal fine, il Titolare adotta un'apposita procedura interna di "*data breach*" che coinvolge i dipendenti del Unione.
Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è "elevato", allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:

a) danni fisici, materiali o immateriali alle persone fisiche;
b) perdita del controllo dei dati personali;
c) limitazione dei diritti, discriminazione;
d) furto o usurpazione d'identità;
e) perdite finanziarie, danno economico o sociale.
f) decifratura non autorizzata della pseudonimizzazione;
g) pregiudizio alla reputazione;
h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. La notifica deve avere il contenuto minimo previsto dall'art. 33 del GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

5. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.

Art. 11 Abrogazione norme unionali previgenti

1. Il presente Regolamento sostituisce integralmente eventuali precedenti Regolamenti della stessa materia.

Art. 12 Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del GDPR e del Codice Privacy, così come novellato dal D. Lgs 101/2018, e s.m.i..

Art. 13 Obbligo di rispetto degli altri Regolamenti unionali

1. Per quanto non espressamente previsto dal presente Regolamento, è fatto obbligo di osservare le disposizioni di tutti gli altri Piani e Regolamenti unionali vigenti.

Art. 14 (Modifiche al presente regolamento)

1. Eventuali modifiche al presente Regolamento debbono essere approvate dal Consiglio dell'Unione