REGOLAMENTO COMUNALE PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

INDICE

Art. 1 – Oggetto	pag.	2
Art. 2 - Titolare del trattamento	pag.	2
Art. 3 - Finalità del trattamento	pag.	3
Art. 4 - Responsabile del trattamento	pag.	3
Art. 5 - Responsabile della protezione dati	pag.	4
Art. 6 - Sicurezza del trattamento	pag.	6
Art. 7 - Registro delle attività di trattamento	pag.	6
Art. 8 - Valutazione d'impatto sulla protezione dei dati	pag.	7
Art. 9 - Violazione dei dati personali	pag.	9
Art. 10 – Riscontro all'esercizio dei diritti degli interessati	pag.	10
Art. 11 – Rinvio	pag.	10

REGOLAMENTO COMUNALE PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Art. 1 Oggetto

Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Cerignola.

Art.2 Titolare del trattamento

Il Comune di Cerignola, rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Sindaco può delegare le relative funzioni a Dirigente/Responsabile P.O. in possesso di adeguate competenze.

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

Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.

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 RGPD, 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.

Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

Il Titolare, inoltre, provvede a:

a) designare i Responsabili del trattamento nelle persone dei Dirigenti/Responsabili P.O. e dei Funzionari delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al

trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;

b) nominare il Responsabile della protezione dei dati;

c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune 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; (in relazione alle dimensioni organizzative del Comune)

d) predisporre l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'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 RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

Il Comune 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 RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art.3 Finalità del trattamento

I trattamenti sono compiuti dal Comune per le seguenti finalità:

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 ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
   - la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
   - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
c) l'esecuzione di un contratto con soggetti interessati;

Art.4 Responsabili del trattamento

Nei casi in cui un soggetto terzo effettua trattamenti di dati personali per conto dell'Ente e non può essere considerato come autonomo Titolare o Contitolare, questi è nominato come **Responsabile esterno trattamento dati** ai sensi dell'art. 28 del Regolamento UE 2016/679.

Sono designati responsabili esterni del trattamento di dati personali, pertanto, i soggetti estranei all'Amministrazione Comunale 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. Qualora occorra affidare un incarico comportante anche trattamenti 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, affinché 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.

Relativamente alla formalizzazione della nomina conseguente a tutte le tipologie di accordi/contratti, ogni delegato/referente di settore ha la responsabilità di garantire che tutti i contratti aventi per oggetto in via diretta o indiretta un trattamento dei dati in nome e per conto dell'Ente contemplino delle specifiche clausole, definite in accordo con il Responsabile Protezione Dati, in cui si prevede la nomina della controparte a Responsabile esterno del trattamento oggetto del contratto. In alternativa il contratto dovrà essere integrato con la lettera di designazione a Responsabile Trattamento dei dati esterno.

Gli atti di incarico devono riportare sinteticamente gli elementi di cui all'art. 28 RGPD; a tal fine, è obbligatorio utilizzare la specifica procedura predisposta (Titolo 7) per la designazione dei responsabili esterni ed i format allegati.

Art.5 Responsabili della Protezione dei Dati

Il Titolare del trattamento ha designato **Responsabile della protezione dei dati** / **Data Protection Officer** (in seguito indicato con "RPD" o "DPO") un soggetto giuridico esterno qualificato ovvero in possesso di esperienza ultra decennale sui temi della Data Protection e della Cyber Security; la scelta di rivolgersi ad una figura esterna all'Ente è dovuta all'assenza di tali specifiche competenze multidisciplinari all'interno dell'Ente e a garanzia di imparzialità, indipendenza ed assenza di conflitto di interesse con le funzioni connesse alla determinazione dei trattamenti effettuati dal Comune (per non far coincidere un soggetto controllore con un soggetto controllato), così come prevede la normativa europea.

Oltre ad essere un obbligo di legge, la nomina del RPD/DPO si configura quale figura essenziale per il rispetto delle nuove norme in materia di protezione dei dati e punto di riferimento per quanti all'interno dell'Ente compiono operazioni di trattamento in qualità di Designati e/o autorizzati.

Il RPD/DPO diventa figura di Garanzia per l'Ente e, pertanto, supporta l'Ente nel miglioramento delle attuali prassi e procedure, al fine di adeguarlo alle normative europee su GDPR e CYBERSECURITY e alle ulteriori norme nazionali.

Il Responsabile Protezione Dati - RPD/DPO è incaricato dei seguenti compiti:

- informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD/DPO può indicare al Titolare e/o al Responsabile del trattamento 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, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
- sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento.

- Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;
- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;
- fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD/DPO in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;
- 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 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD/DPO è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;
- supportare il Dirigente Responsabile dei Servizi di Sicurezza nella valutazione e nella scelta delle soluzioni hardware e software, in particolar modo applicativi gestionali destinati al trattamento di dati personali, per quanto attinente la verifica dei requisiti di sicurezza (art. 25 e 32 del GDPR) ed esprimere parere in merito;
- supportare il Dirigente Responsabile dei Servizi di Sicurezza per quanto attiene a valutazioni, acquisizioni, di soluzioni infrastrutturali e per la Cyber Security;
- supportare il Dirigente Responsabile dei Servizi di Sicurezza per quanto attiene a valutazioni, acquisizioni o sviluppo di portali pubblici (siti Internet, extranet, Intranet, Cloud, etc);
- altri compiti e funzioni a condizione che il Titolare o il Delegato/Referente di settore si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi.
- L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD/DPO.

Il RPD/DPO opera a stretto contatto con il Dirigente Responsabile dei Servizi di Sicurezza per tutte le questioni che attengono la protezione dei dati e la sicurezza. In particolare, tutto ciò che impatta sulla sicurezza deve essere posto al vaglio del RPD/DPO e il personale interno preposto al trattamento deve portare all'attenzione del RPD/DPO la necessità di introdurre un nuovo trattamento o l'affidamento di un servizio a responsabili esterni all'Ente.

Il Titolare del trattamento assicura che il RPD/DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD/DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD/DPO deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD/DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD/DPO, è necessario motivare specificamente tale decisione;

- il RPD/DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Art.6 Sicurezza del Trattamento

L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche.

Il Titolare del trattamento mette in atto, con l'ausilio del Dirigente Responsabile dei Servizi di Sicurezza, a cui viene delegata la definizione e l'attuazione, misure tecniche ed organizzative adeguate per 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.

Il Dirigente Responsabile dei Servizi di Sicurezza si avvale del RPD/DPO per la valutazione delle misure di sicurezza ex art.32 del GDPR e dell'Amministratore del sistema informatico interno o dell'eventuale società di servizi IT per l'attuazione.

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.

Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Delegato/Referente di settore del trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro), back up e procedure di disaster recovery (business continuity;
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

L'introduzione, la modifica, la dismissione, l'implementazione o qualunque azione che riguardi applicativi (o applicazioni) che trattano o che possano trattare dati personali e/o strumenti che influenzino o possano influenzare i livelli di sicurezza dei sistemi informativi dell'Ente e della relativa infrastruttura, prima di essere introdotti, modificati, implementati o dismessi, sono ammessi solo su parere positivo del Dirigente Responsabile dei Servizi di Sicurezza, che può anche delegarne la gestione, sentito il RPD/DPO.

La conformità del trattamento dei dati al RGDP 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.

Il Titolare e ciascun Delegato/Referente di settore del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

Art.7 Il Registro dei Trattamenti

Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato, presso gli uffici della struttura organizzativa dell'Ente in forma telematica/cartacea.

Il Titolare del trattamento affida al RPD/DPO il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare, salvo diversa valutazione.

Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

- il nome ed i dati di contatto dell'Ente, degli eventuali Contitolari del trattamento e del RPD/DPO;
- le finalità del trattamento;
- la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Ogni Delegato verifica, per la parte (settore) di propria competenza, la correttezza e completezza delle informazioni inserite e ad aggiornare il Registro laddove necessario.

Art. 8 Valutazione d'impatto sulla protezione dei dati

Nel caso in cui un tipo di trattamento, specie se prevede in particolare 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 attuare una **valutazione dell'impatto** del medesimo trattamento (**DPIA**) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

Il Titolare deve consultarsi con il RPD/DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate.

Il Regolamento richiede di procedere ad una valutazione d'impatto qualora si valuti che un trattamento "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*". A questo proposito, il gruppo di lavoro articolo 29 sulla protezione dei dati (WP29), elenca 9 criteri da tenere in considerazione nello svolgimento di tale valutazione. Il soddisfacimento di almeno due dei 9 criteri elencati è indice di un trattamento "*ad alto rischio per i diritti e le libertà dell'interessato*" quindi della necessità di una valutazione riguardo il suo impatto sui dati personali come di seguito dettagliato:

- trattamenti valutativi o di scoring (compresa la profilazione, il tracciamento delle preferenze dell'interessato, della sua ubicazione o dei suoi spostamenti);
- decisioni automatizzate che producono significativi effetti giuridici o di analoga natura (anche trattamenti che possano portare all'esclusione o alla discriminazione degli interessati);

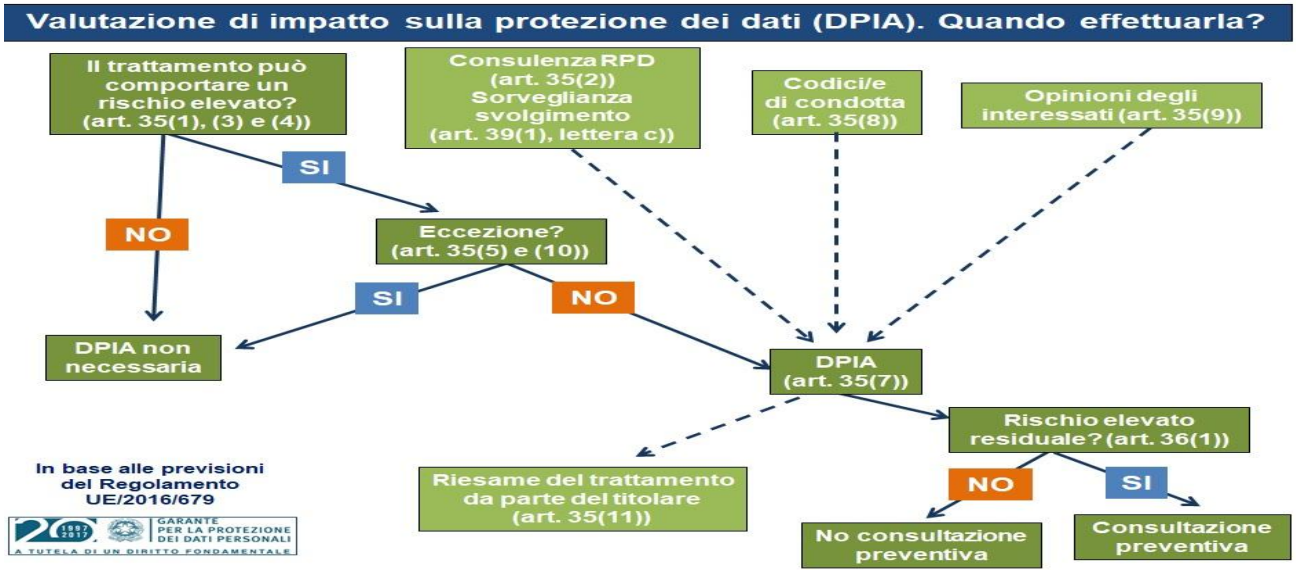
- monitoraggio sistematico (compresa "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico";
- trattamento di dati sensibili o di dati di natura estremamente personale (dati di natura particolare di cui all'art. 9 del GDPR e dati relativi a condanne penali o a reati di cui all'art. 10 dello stesso Regolamento;
- trattamenti di dati su larga scala (da considerare il numero di interessati coinvolti, il volume dei dati, l'area geografica di riferimento, la durata);
- combinazione o raffronto di insiemi di dati (ad es. a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi…);
- trattamenti di dati relativi a interessati vulnerabili (i minori, i dipendenti, i segmenti più vulnerabili della popolazione e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (quali ad es. "la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici");
- impedimenti (per gli interessati) di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Solitamente si procede a una valutazione d'impatto sulla protezione dei dati relativamente ad una singola operazione di trattamento dati, tuttavia l'art. 35 del GDPR ammette anche che *"…una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*".

Una volta effettuato il paragone con i criteri sopra riportati deve essere operata una valutazione specifica caso per caso da parte del responsabile della funzione delegata al trattamento: in alcune situazioni un trattamento può, infatti, trovare corrispondenza con i criteri considerati "rischiosi" ma allo stesso tempo essere considerato dal titolare del trattamento tale da non "presentare un rischio elevato". In tali casi è comunque opportuno che il titolare del trattamento giustifichi e documenti i motivi che lo hanno spinto a non effettuare una valutazione d'impatto sulla protezione dei dati, includendo/registrando i punti di vista del responsabile della protezione dei dati.

Il WP29 raccomanda, nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, "di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati".

La scelta finale sull'esecuzione della DPIA spetta al Titolare del trattamento, opportunamente consigliato in materia da parte del DPO.



Una volta che il Titolare (con il supporto del RPD/DPO) ha deciso che un trattamento deve essere oggetto di DPIA, al Responsabile della funzione delegata al trattamento è assegnata la responsabilità di esecuzione della medesima con annessa definizione di strumenti da impiegare e tempistica.

Art.9 Violazione dei dati personali

Per violazione dei dati personali (in 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 dall'Ente.

Possiamo considerare realizzata una violazione di dati nei seguenti casi:

- Lettura (presumibilmente i dati non sono stati copiati);
- Copia (i dati sono ancora presenti sui sistemi del titolare);
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati);
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione);
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione).

Il personale addetto al trattamento qualora venga a conoscenza, nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi di eventuali violazioni dei dati personali o di incidenti di sicurezza che possano esporre a rischio di violazione dei dati (data breach) deve tempestivamente informare il Titolare, attraverso il Referente Privacy Interno (delegato) o il Responsabile della Protezione dei Dati.

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*, utilizzando la procedura operativa predisposta.

Anche l'eventuale Responsabile esterno del trattamento nominato è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione entro 24

ore. E' opportuno, pertanto, che ciascun contratto di servizi prevede clausole specifiche al riguardo.

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

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

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.

Art.10 Riscontro all'esercizio dei diritti degli interessati

Ogni responsabile di settore, in collaborazione del Responsabile Protezione Dati, ha la responsabilità di gestire le richieste da parte degli interessati pervenute all'Ente relativamente alle casistiche identificate dagli artt. 15-22 e seguenti del Regolamento UE 2016/679, utilizzando la procedura operativa predisposta.

Il Responsabile di settore, in collaborazione con il Responsabile della Protezione dei Dati, deve assicurare che l'interessato riceva riscontro alla sua richiesta entro 30 giorni. A tal fine il Responsabile di settore è supportato:

- dall'ufficio competente;
- dagli esperti legali per definire il testo della risposta;
- dagli outsourcee per raccogliere i dati personali, eventualmente trattati dai sistemi informatici, necessari a fornire il riscontro richiesto.

Per il riscontro degli interessati utilizzare la procedura operativa (Titolo 4 "Procedura per l'esercizio dei nuovi diritti") e la relativa modulistica predisposta.

Art.11 Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.