COMUNE DI PATERNO

REGOLAMENTO COMUNALE PER L'ATTUAZIONE/APPLICAZIONE DEL REGOLAMENTO UE 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO DEL 17 APRILE 2016 RELATIVO ALLA PROTEZIONE DEI DATI

Art. 1

Oggetto

Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio che devono essere applicate nel Comune di Paterno, ai fini di garantire la piena efficacia e la più efficiente attuazione del Regolamento europeo 2016/679 (Regolamento Generale Protezione dei dati – *breviter* RGPD) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Art. 2

Finalità del trattamento

Il Comune di Paterno effettua il trattamento dei dati per le seguenti finalità:

1) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri tra cui rientrano:

a) 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;
b) la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
c) l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

2) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
3) l'esecuzione di un contratto con soggetti interessati;
4) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato presti validamente il consenso al trattamento.

Il trattamento dei dati deve, sempre, essere effettuato secondo la finalità teleologica stabilita dalla legge per il trattamento stesso.

Art. 3

Titolare del trattamento

Il Comune di Paterno (*breviter* Titolare), nella persona del Sindaco *pro tempore*, è il Titolare del trattamento dei dati personali effettuato sia, integralmente o parzialmente, secondo modalità automatizzate e sia mediante l'inserimento dei dati in archivi cartacei.

Il Titolare è responsabile affinchè i dati vengano trattati secondo i principi di liceità, corretta informazione, esattezza, integrità e riservatezza, minimizzazione dei dati, limitazione della finalità e della conservazione dei dati trattati (RGDP, art. 5, n.1).

Il Titolare adotta le informative nella forma appropriata al dato trattato il cui contenuto deve essere espresso in modo coinciso, trasparente, intellegibile per l'interessato e facilmente accessibile.

Il Titolare adotta informative idonee, espresse in modo chiaro e semplice, per i minori.

Per il contenuto delle informative, a seconda che il dato venga acquisito o meno presso l'interessato si fa rinvio *per relationem* agli artt. 13 e 14 del RGPD.

Art. 4

Obblighi del titolare del trattamento

Il Titolare deve effettuare una valutazione dell'impatto del trattamento effettuato, in particolare, mediante l'uso di nuove tecnologie, sulla protezione dei dati personali quando il trattamento possa presentare un rischio elevato, in considerazione della natura, dell'oggetto, del contesto e delle finalità del medesimo trattamento, per i diritti e le libertà delle persone fisiche (art. 35 del RGPD).

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.

Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio 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.

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.

Il Comune di Paterno, inoltre, favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli altri organismi rappresentativi della categoria dei titolari o dei rappresentanti del trattamento, ovvero a meccanismi di certificazione della protezione dei dati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare del trattamento.

Art. 5

Responsabile del trattamento

Il Titolare, nella persona del Sindaco p.t., può delegare le relative funzioni al Dirigente/Responsabile P.O. in possesso di adeguate competenze, predisponendo e pubblicando sul sito istituzionale, altresì, l'elenco dei responsabili e sub responsabili del trattamento delle strutture in cui è organizzato il Comune.

I responsabili del trattamento possono essere nominati mediante Decreto del Sindaco, nel quale deve essere tassativamente indicata:

a) la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
b) il tipo di dati personali oggetto di trattamento e le categorie di interessati;
c) gli obblighi ed i diritti del Titolare del trattamento.

Se la delega della funzione di responsabile del trattamento avviene a favore di soggetti esterni essa deve avere la forma di un contratto di altro atto giuridico riconosciuto dall'ordinamento giuridico italiano o unionale e deve contenere quanto previsto dall'art. 28, n. 3, del RGPD.

Il Responsabile 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 del registro delle categorie di attività di trattamento svolte per conto del Titolare;
b) all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
c) alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;

a) Informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione europea relative alla protezione dei dati.
b) Sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.
c) Fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del RGPD.
d) Cooperare con il Garante per la protezione dei dati personali.
e) Fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva, di cui all'art. 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione non in conflitto con il ruolo rivestito.
f) Garantire la conservazione della documentazione relativa ai trattamenti effettuati dal titolare (registri).

Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

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

a) il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali.
b) il RPD 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.
c) il parere del RPD 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, è necessario motivare specificamente tale decisione.
d) il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD. La figura di RPD è incompatibile con chi determina le finalità o i mezzi del trattamento, in particolare, risultano incompatibili con il ruolo di RDP:

- il Responsabile per la prevenzione della corruzione e per la trasparenza
- il Responsabile del trattamento
- qualunque altro incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

Il Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare, è assicurato al RPD:

a) supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e della Giunta comunale, 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 affidati al RPD.
c) supporto adeguato in termini di risorse finanziarie, infrastrutture.
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.

Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti, in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Sindaco o suo delegato - od al Responsabile del trattamento.

Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

Art. 8

Sicurezza del trattamento

Il Comune di Paterno e ciascun Responsabile del trattamento mettono in atto 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.

Tra le misure tecniche ed organizzative di sicurezza che possono essere messe in atto per ridurre i rischi del trattamento vi sono 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 Responsabile del trattamento: i sistemi di autenticazione, i sistemi di autorizzazione, sistemi di protezione (antivirus; firewall; antintrusione; altro), sistemi di protezione con videosorveglianza, registrazione accessi.

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 Comune di Paterno e ciascun Responsabile 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.

I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.

Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico.

Art. 9

Registro delle attività del trattamento

Il Titolare del trattamento istituisce il registro delle attività del trattamento.

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

a) il nome ed i dati di contatto del Comune, del Sindaco e/o del suo Responsabile e del RPD

b) le finalità del trattamento

c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati

e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati

Il Registro è tenuto dal Titolare, ovvero dal soggetto dallo stesso delegato, ovvero può essere affidato al RDP, presso gli uffici della struttura organizzativa del Comune in forma telematica/cartacea, sotto la responsabilità del medesimo Titolare.

Art. 10

Registro delle categorie di attività trattate

Il Titolare del trattamento istituisce il registro delle categorie attività trattate.

Il Registro delle categorie di attività trattate da ciascun Responsabile reca le seguenti informazioni:

a) il nome ed i dati di contatto del Responsabile del trattamento e del RPD.

b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali.

c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale.

d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica o cartacea.

Il Responsabile del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile.

Art. 11

Valutazione di 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 (*breviter* 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.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'at. 35, paragrafi 4-6 del RGPD.

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, p. 3, RGDP, 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

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP

e) trattamenti di dati su larga scala, tenendo conto: del numero di 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, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori

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 almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

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 Comune. Il Titolare deve consultarsi con il RPD 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 RPD monitora lo svolgimento della DPIA.

Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

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.

Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. 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.

La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica.

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) 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) 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 limitato di conservazione; delle informazioni fornite agli interessati

- del diritto di accesso e portabilità dei dati

- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento

- dei rapporti con i responsabili del trattamento

- delle garanzie per i trasferimenti internazionali di dati

- consultazione preventiva del Garante privacy

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

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.

Art. 12

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 dal Comune.

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. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

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:

- 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 ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati
- riguardare categorie particolari di dati personali
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze).
- comportare rischi imminenti e con un'elevata probabilità di accadimento
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

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

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 RGPD.

Art. 13

Rinvio

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD 2016/679 e tutte le norme di attuazione vigenti.