

REGOLAMENTO TRATTAMENTO DEI DATI PERSONALI

Approvato con deliberazione del Consiglio dell'Unione n. 9 del 28/04/2023 esecutiva ai sensi di legge.

INDICE

Articolo 1 - Oggetto
Articolo 2 - Titolare del trattamento
Articolo 3 - Finalità del trattamento dati personali
Articolo 4 - Designati/e / Autorizzati/e
Articolo 5 - Responsabile esterno/a
Articolo 6 - Responsabile della protezione dati
Articolo 7 - Organizzazione Interna / Ufficio Privacy / Referenti
Articolo 8 - Sicurezza del trattamento
Articolo 9 - Registro unico delle attività di trattamento
Articolo 10 - Altri registri
Articolo 11 - Valutazioni d'impatto sulla protezione dei dati
Articolo 12 - Violazione dei dati personali
Articolo 13 - Particolari categorie di dati
Articolo 14 - Rinvio

Articolo 1 - Oggetto

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

Articolo 2 - Titolare del trattamento

1. L'Unione di Comuni Vini e Tratufi., rappresentata ai fini previsti dal RGPD dal Presidente 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 Presidente può designare per specifici compiti e funzioni i/le Dirigenti dell'ente con specifico provvedimento.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dalla normativa europea: 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 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 dalla normativa europea, 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 adotta misure appropriate per fornire all'interessato/a:

- a) le informazioni indicate dall'articolo 13 RGPD, qualora i dati personali siano raccolti presso lo/la stesso/a interessato/a;
- b) le informazioni indicate dall'articolo 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo/la stesso/a interessato/a.

5. 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 della normativa europea, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 9.

6. Il Titolare inoltre:

- a) designa per specifici compiti e funzioni i/le dirigenti preposti/e alle strutture in cui si articola l'organizzazione dell'Ente;
- b) nomina il/la Responsabile della protezione dei dati.

Articolo 3 - Finalità del trattamento dati personali

1. I trattamenti relativi ai dati personali sono compiuti dall'Unione per le seguenti finalità:
 - a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
 - b) l'adempimento di un obbligo legale al quale è soggetta l'Unione. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
 - c) l'esecuzione di un contratto con soggetti interessati.

2. I trattamenti di particolari categorie di dati sono compiuti, se previsti dal diritto dell'Unione Europea o da disposizione di legge, per motivi di interesse pubblico rilevante, proporzionato alla finalità perseguita, come individuati dalla legge.

3. Con riguardo ai dati relativi a condanne penali o reati, il trattamento è consentito solo se autorizzato da norma di legge.

4. Fuori dai casi previsti dal comma 1, il trattamento è ammesso solo se l'interessato/a presta il proprio consenso.

Articolo 4 - Designati/e / Autorizzati/e

1. Ai/alle Dirigenti possono essere attribuiti specifici compiti e funzioni connessi al trattamento dei dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. I/le designati/e garantiscono adeguata conoscenza specialistica.

2. Il/la Designato/a provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidati dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
 - alla predisposizione e al mantenimento del Registro dei trattamenti;
 - all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
 - alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
 - ad individuare, contrattualizzare e nominare i/le responsabili di trattamento esterni, nel rispetto delle procedure di cui alla normativa europea;
 - a definire le informative per gli/le interessati/e che dovranno essere realizzate ed apposte in calce alla modulistica ovvero ai servizi on line ovvero affisse nei luoghi di ricevimento del pubblico;
 - a determinare, ove necessario, un/una referente interno/a per le questioni operative relative agli adempimenti del Regolamento Europeo e delle norme nazionali e locali (ivi

inclusi i regolamenti comunali), nonché per monitorare l'applicazione corretta delle norme all'interno dell'area di competenza; il/la referente potrà essere condiviso a livello aggregato qualora ciò sia compatibile con la complessità e l'omogeneità dei trattamenti presenti;

- ad interloquire e collaborare con il/la Responsabile della protezione dati ed ad attuare prescrizioni e raccomandazioni, ove possibili, emerse in sede di audit interni;
- a predisporre, in accordo con il/la Responsabile protezione dati, un calendario di audit da svolgere congiuntamente, nei confronti dei/delle responsabili esterni/e nominati/e, anche a campione ovvero a rotazione;
- a svolgere, per la parte di competenza, l'analisi d'impatto nei casi ove essa è obbligatoria o comunque significativa in ordine alla corretta gestione dei trattamenti, anche dopo avere consultato il/la Responsabile Protezione dati;
- a svolgere l'attività preliminare a seguito di ipotesi di perdita di dati (data breach) di cui viene a conoscenza, informandone anche il gruppo di crisi "data breach" se già operativo, ed inoltrare la notifica al Garante, sentito, ove il caso, anche il/la Responsabile Protezione dati; di dette violazioni dovrà darsi conto in un apposito "registro delle violazioni", che confluirà in un registro unico a livello di ente.

3. I/le dipendenti dell'Unione, sono autorizzati/e dal Designato/a competente al trattamento dei dati riferiti alla struttura di riferimento come individuati/e nel rispettivo registro dei trattamenti, con il quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati/e;
- gli obblighi ed i diritti del/della Titolare del trattamento;
- le misure di sicurezza in rapporto ai rischi.

Ai/alle dipendenti autorizzati/e verranno fornite specifiche istruzioni.

Articolo 5 - Responsabile esterno/a

1. Il/la Designato/a può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati che, in qualità di responsabili esterni/e del trattamento, forniscano le garanzie di cui al comma 1 dell'articolo 4, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del/della responsabile del trattamento e le modalità di trattamento.

Gli atti che disciplinano il rapporto tra il/la Designato/a ed il/la responsabile esterno/a del trattamento devono in particolare contenere quanto previsto dalla normativa europea.

2. Il/la Responsabile esterno/a del trattamento non ricorre ad altro/a responsabile senza previa autorizzazione scritta, specifica o generale, del designato/a del trattamento, contenuta

nell'atto di nomina, e comunque nel rispetto degli obblighi contrattuali che lo/la legano al/alla Designato/a. In caso di autorizzazione scritta generale, il/la responsabile esterno/a informa in ogni caso il/la designato/a della nomina o sostituzione di sub-responsabili dando così al/alla designato/a l'opportunità di opporvisi. Nei confronti del/della Designato/a risponde sempre e comunque il/la responsabile primario/a per le inadempienze o le violazioni causate dall'attività dei/delle sub-responsabili, anche ai fini del risarcimento degli eventuali danni causati dal trattamento, salvo che dimostri che l'evento dannoso non gli è in alcun modo imputabile o che ha vigilato in modo adeguato sull'operato del/della sub-responsabile. Le operazioni di trattamento possono essere effettuate solo da incaricati/e autorizzati/e che operano sotto la diretta autorità del/della Responsabile esterno/a attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

Articolo 6 - Responsabile della protezione dati

1. Il/La Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato/a nella figura unica di un/una dipendente di ruolo dell'Unione o di un Comune che vi partecipa ovvero in un soggetto esterno scelto tramite procedura ad evidenza pubblica. L'atto di designazione determinerà la durata dell'incarico.

Il/La RPD è incaricato/a dei seguenti compiti:

- a) informare e fornire consulenza al Titolare ed ai/alle designati/e nonché ai/alle 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/la RPD può indicare al Titolare e/o ai/alle designati/e 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;
- b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del/della designato/a. 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/della Responsabile del trattamento;
- c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal/dalla Designato/a;
- d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il/la designato/a, in particolare, si consulta con il/la RPD in merito a condurre o meno la valutazione; quale metodologia adottare nel condurla; condurre la valutazione con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la valutazione 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;
- 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 prevista dalla normativa europea, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del/della RPD è comunicato dal Titolare e/o dal/dalla designato/a al Garante;
 - f) altri compiti e funzioni a condizione che il Titolare o il/la Designato/a al trattamento 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/della RPD;
 - g) svolgere altresì i compiti di RPD con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati;
2. Il Titolare ed il/la Designato/a al trattamento assicurano che il/la RPD sia tempestivamente e adeguatamente coinvolto/a in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
- il/la RPD è invitato/a a partecipare alle riunioni di coordinamento Referenti privacy, che abbiano per oggetto questioni inerenti la protezione dei dati personali;
 - il/la 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;
 - il parere del/della RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determini condotte difformi da quelle raccomandate dal/dalla RPD, è necessario motivare specificamente tale decisione;
 - il/la RPD deve essere consultato/a tempestivamente qualora si verifichi una violazione dei dati (o un altro incidente).
3. La figura del/della RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
- il/la Responsabile per la prevenzione della corruzione e per la trasparenza/R.T. (ove diverso);
 - il/la Designato/a al trattamento;
 - qualunque incarico o funzione che comporti la determinazione di finalità o mezzi del trattamento.
4. Il Titolare fornisce al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti:

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

5. Il/la RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti.

Il/la RPD non può essere rimosso/a o penalizzato/a dal Titolare e dai/dalle designati/e del trattamento in ragione dell'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il/la RPD riferisce direttamente al Titolare od ai/alle designati/e del trattamento.

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

Articolo 7 – Organizzazione Interna / Ufficio Privacy / Referenti interni/e

1. Nell'ambito della struttura organizzativa dell'ente, è costituito un “Ufficio privacy”, con il compito di coordinare la gestione operativa degli adempimenti in materia di privacy dell’Unione e dei singoli Comuni nonché di curare gli approfondimenti normativi e verificare l'applicazione del presente regolamento. L’ufficio è composto dai soggetti di cui al comma secondo del presente articolo, il Segretario dell’Unione ed è coordinato dal designato RDP.

2. Ciascun Comune dell’Unione individua un/una proprio/a referente per le questioni operative relative agli adempimenti del RGPD e delle norme nazionali e del presente regolamento, nonché per monitorare l'applicazione corretta delle norme all'interno della struttura di riferimento.

3. Il Gruppo di lavoro “Ufficio Privacy” viene costituito anche con funzioni di “Gruppo di lavoro per emergenza DATA BREACH”.

4. In assenza di formale designazione, coloro che trattano dati personali nell’ambito del rapporto con la l’Amministrazione sono comunque ritenuti autorizzati al trattamento dei dati personali e sono obbligati a osservare quanto previsto dal presente Regolamento.

5. L’Unione, nel rispetto del presente Regolamento e quale migliore strategia volta a presidiare i trattamenti dei dati effettuati, può dotarsi di un modello organizzativo in materia di protezione dei dati personali che definisca i criteri generali da rispettare nell’individuazione dei soggetti incaricati, a compiere operazioni di trattamento nonché le procedure da adottare per evitare il rischio di diffusione, accesso incontrollato o corruzione dei dati a qualunque titolo gestiti o detenuti dall’Ente.

Articolo 8 - Sicurezza del trattamento

1. L'Unione e ciascun/a Designato/a mettono in atto misure tecniche ed organizzative idonee 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 tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun designato:
 - sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
 - 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.
4. 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.
5. L'Unione e ciascun/ciascuna Designato/a si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
6. I nominativi ed i dati di contatto del Titolare e del/della Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'Ente, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.

Articolo 9 - Registro delle attività di trattamento

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

- a) il nome ed i dati di contatto dell'Ente,
- b) attività e loro descrizione;
- c) le finalità del trattamento;
- d) base giuridica;
- e) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- f) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- g) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- h) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente articolo 6.

2. Attese le dimensioni organizzative, l'Ente ha scelto di istituire un registro unico dei trattamenti e dei rischi che contiene tutte le informazioni di cui al presente articolo e quelle di cui al successivo.

3. Il Registro Unico è tenuto dall'Ente in forma telematica/cartacea sotto la responsabilità del soggetto Designato nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.

Articolo 10 - Altri Registri

1. L'Unione deve formare e detenere un registro dei/delle responsabili esterni/e nominati/e in relazione alle attività svolte per conto del Titolare. Il registro deve contenere almeno:

- il nome e i dati di contatto del/della responsabile esterno/a del trattamento;
- gli estremi identificativi del contratto di nomina (o analogo), decorrenza e scadenza, determinazione di affidamento, della nomina;
- alla scadenza del contratto il registro terrà traccia dell'avvenuta cancellazione dei dati da parte del/della Responsabile esterno/a se a suo tempo conferiti, riportando data ed esito positivo del rientro degli archivi cartacei o digitali;
- il riferimento al registro dei trattamenti per il quale è stato nominato/a responsabile esterno/a;
- eventuale autorizzazione generale o specifica ed elencazione dei/delle sotto-responsabili nominati/e.

2. L'Unione detiene un diario delle attività svolte in tema di protezione dati personali, ivi annotando tutte le richieste di accesso a lui/lei pervenute e relativo esito, riportando i dati identificativi della richiesta, una breve descrizione e le azioni svolte, inclusa l'eventuale motivazione e di diniego totale o parziale. Nello stesso diario annota le attività svolte e le azioni intraprese (formazione, azioni conseguenti ad audit, eccetera) con l'obiettivo di dare conto di tutta l'attività in materia.

Articolo 11 - Valutazioni d'impatto sulla protezione dei dati

1. 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 della normativa europea, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La Valutazione è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la valutazione si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi del RGDP.

Articolo 12 - Violazione dei dati personali

1. 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'Unione

2. Il Titolare / Il/la designato/a, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, informa il gruppo di emergenza di cui all'articolo 7 e provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Designato/Responsabile esterno del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al 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).

4. Se il Titolare / il/la designato/a ritiene che il rischio per i diritti e le libertà degli/delle interessati/e conseguente alla violazione rilevata è elevato, allora deve informare questi/e ultimi/e, senza ingiustificato 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 (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

5. La notifica deve avere il contenuto minimo previsto dal RGPD, ed anche la comunicazione all'interessato/a deve contenere almeno le informazioni e le misure previste.

6. Il Titolare / Il/la designato/a 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.

Articolo 13 - Particolari categorie di dati

1. Le particolari categorie di dati trattati nell'ambito delle attività di pertinenza degli uffici e servizi in cui si articola l'ente sono descritte in apposite schede, allegate ai registri dei Designati/e e nel Registro complessivo dell'ente.

2. Essi sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi mentre le operazioni di interconnessione, raffronto, comunicazione e diffusione individuate nelle schede sono ammesse soltanto se indispensabili allo svolgimento degli obblighi e compiti di volta in volta indicati, per il

perseguimento delle rilevanti finalità di interesse pubblico specificate e nel rispetto dei limiti stabiliti dalle leggi e dai regolamenti.

Articolo 14 - Rinvio

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