

Regolamento (Disposizioni) per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Art. 1 - Oggetto

1. Il presente Regolamento ha lo scopo disciplinare i ruoli, le responsabilità e le modalità attuative finalizzate all'applicazione dei principi e delle prescrizioni contenute nel Regolamento generale sulla protezione dei dati personali approvato con deliberazione del Consiglio d'Europa del 27 aprile 2016 n. 679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, nonché alle disposizioni contenute nel Codice della privacy, approvato con il decreto legislativo 30 giugno 2003, n. 196 e modificato con il decreto legislativo 10 agosto 2018, n.101.

Art. 2 - Titolarità del trattamento

1. In conformità agli articoli 4, punto 7) del Regolamento europeo, sopra richiamato, il Titolare del trattamento è l'Unione di Comuni montana Colline Metallifere che, ai sensi dell'articolo 24, comma 1 del regolamento UE, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.
2. Il Titolare, sopra individuato, è responsabile del rispetto dei principi prescritti dal Regolamento Generale e in particolare di quanto previsto dall'art. 5 del citato Regolamento europeo con riferimento alla liceità, correttezza e trasparenza nel trattamento, nonché la limitazione e minimizzazione dei dati, la loro esattezza e la conservazione avendo cura di assicurarne l'integrità e il rispetto della riservatezza.
3. Il Titolare promuove l'adozione delle misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali sia effettuato in modo conforme al RGPD, anche attraverso la definizione di specifici ruoli e responsabilità.
4. Il Titolare, inoltre, organizza la vigilanza e il presidio sull'adozione delle misure allo scopo di assicurare, sia la protezione dei dati, sia l'esercizio dei diritti degli interessati, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. A tal fine provvede a:
 - a) designare, ai sensi dell'articolo 28 del dlgs 196/2003 e dell'articolo 37 del Regolamento UE 2016/679 un Responsabile della protezione dati, individuandolo tra i professionisti esterni che siano in possesso dei requisiti di esperienza e professionalità, anche ricorrendo all'affidamento del servizio a soggetti esterni che assicurino l'espletamento delle attività necessarie all'attuazione concreta delle disposizioni del Regolamento generale;
 - b) designare, ai sensi dell'articolo 2-quaterdecies del dlgs 196/2003 quali Responsabili interni del trattamento i Dirigenti e gli incaricati di Elevata Qualificazione dei Settori e Servizi in cui si articola l'Ente;
 - c) incaricare i Dirigenti e gli incaricati di Elevata Qualificazione dei Settori e Servizi, laddove si ricorra all'affidamento all'esterno di servizi che richiedano il trattamento di dati personali, di definire gli ambiti e i ruoli in ordine alla Responsabilità esterna del trattamento, mediante la specifica prescrizione dei relativi obblighi e delle garanzie richieste, in sede contrattuale;
 - d) definire, all'interno dell'ente, i ruoli e le responsabilità in materia di trattamento di dati personali, sia prevedendo specifiche attribuzioni formali, sia come diretta conseguenza dell'appartenenza a un ufficio o per l'espletamento di compiti specifici;
 - e) definire, nel caso di servizio associato di funzioni, gli ambiti di responsabilità del trattamento dei dati, sia all'interno dell'ente, sia all'esterno.

5. Al Titolare del trattamento compete inoltre l'adozione di codici di condotta che disciplinino l'esecuzione delle attività nel rispetto del corretto trattamento dei dati, nonché 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.
6. Ai sensi dell'articolo 30 del Regolamento UE 2016/679, il Titolare è obbligato a tenere un registro dei trattamenti svolti dall'Ente che abbiano carattere di trasversalità.

Art.3 - Finalità del trattamento

1. Il trattamento dei dati personali da parte del Titolare, così come prima definito, ai sensi dell'articolo 2-ter del d. lgs 196/2003, è sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esso attribuiti.
2. La finalità del trattamento, se non espressamente prevista da una norma di legge, deve essere indicata in coerenza al compito svolto o al potere esercitato, assicurando adeguata pubblicità dell'identità del titolare del trattamento, delle finalità del trattamento e fornendo ogni altra informazione necessaria ad assicurare un trattamento corretto e trasparente con riguardo ai soggetti interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.
3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, sono ammesse unicamente se previste da disposizioni legislative o regolamentari.
4. I dati personali che l'Ente acquisisce, sia in forma cartacea che informatica, saranno trattati esclusivamente per le finalità istituzionali, nel rispetto dei principi di correttezza, liceità, trasparenza e di tutela della riservatezza, secondo le prescrizioni contenute nel Regolamento Generale per la protezione dei dati personali, nonché delle disposizioni legislative italiane e delle indicazioni fornite dall'Autorità Garante della protezione dei dati personali.

Art.4 – Modalità di trattamento

1. Il Titolare del trattamento, tenuto conto delle cognizioni tecniche disponibili, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del grado di rischio per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio di violazione dei dati.
2. Il trattamento dei dati, all'interno dell'ente, è effettuato esclusivamente da soggetti esplicitamente e formalmente autorizzati mediante regolamento, atti di designazione, disposizioni contrattuali o la prescrizione di obblighi nel rispetto dei codici di comportamento vigenti.
3. Per il trattamento automatizzato il titolare, previa valutazione dei rischi, adotta misure volte a:
 - a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);
 - b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);
 - c) impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);
 - d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);
 - e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);

- f) garantire la possibilità di individuare i soggetti ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);
 - g) garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);
 - h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);
 - i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);
 - l) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).
4. Le informazioni personali, in nessun caso saranno fornite a soggetti terzi al di fuori dell'esercizio di funzioni pubbliche, fatte salve le prescrizioni di legge. Potrà essere consentita la divulgazione o l'accesso esclusivamente nel rispetto delle prescrizioni normative e delle specifiche procedure e per le finalità consentite dalle leggi vigenti. In ogni caso debbono essere rispettati i principi di liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, limitazione della conservazione, integrità, riservatezza e responsabilizzazione.
 5. L'acquisizione, la conservazione, l'elaborazione, la divulgazione dei dati o l'accesso a soggetti terzi è consentito esclusivamente nel rispetto delle prescrizioni normative e delle modalità attuative, da soggetti espressamente e formalmente autorizzati, nonché informati sulle disposizioni e le misure da attuare, che dovranno operare nel rispetto degli obblighi relativi al trattamento dei dati personali.
 6. In caso di divulgazione di dati personali in ottemperanza alle prescrizioni normative, compete al funzionario che trasmette gli atti ai fini della pubblicazione l'onere di verificarne la correttezza e la coerenza riguardo al trattamento dei dati personali.

Art.5- I Responsabili del trattamento

1. Il dirigente e gli incaricati di Elevata Qualificazione dei Settori e Servizi dell'Ente, in ragione del ruolo rivestito, ai sensi dell'articolo 2-quaterdecies del d.lgs 196/2003, sono designati automaticamente con l'atto di nomina, Responsabili del trattamento nell'ambito delle funzioni ad essi attribuite.
2. Ogni Responsabile del trattamento, di cui al comma precedente, ai sensi dell'articolo 28 del Regolamento UE 2016/679, ha il compito di:
 - a) adottare le misure tecniche e organizzative adeguate affinché, nell'ambito di competenza, i dati personali siano trattati nel rispetto dei principi di liceità, correttezza, minimizzazione, responsabilizzazione, trasparenza, integrità, riservatezza, limitazione della conservazione;
 - b) assicurare la conservazione dei dati in modo da garantirne la loro integrità e limitarne l'accesso e la divulgazione ai soli casi in cui ciò sia autorizzato da norme di legge, nel rispetto delle informazioni dovute ai controinteressati, anche ricorrendo a soggetti terzi che offrano le medesime garanzie e ottemperino ai medesimi obblighi;
 - c) adottare le misure e le prescrizioni previste ai fini del contenimento dei rischi di violazione dei dati personali, nel rispetto delle indicazioni fornite dal Titolare del trattamento e dal Responsabile della protezione dei dati (DPO), al fine di soddisfare gli obblighi prescritti nel Regolamento europeo 679/2016, oltre alle disposizioni del Garante per il trattamento dei dati personali;
 - d) rispondere direttamente nel caso in cui alcuna delle violazioni sia attribuibile alla gestione dei dati di sua competenza, con particolare riguardo ai casi di indebita distruzione, cancellazione, accesso, modifica o divulgazione dei dati personali trattati;

- e) informare immediatamente il Titolare del trattamento e il Responsabile della protezione dei dati individuato dall'Ente, nel caso in cui si verifichi il sospetto di una violazione del trattamento dei dati personali;
 - f) assicurare al Titolare del trattamento l'accesso a qualsiasi informazione, dato o documento relativo al Settore/Servizio affidato;
 - g) adottare ogni idonea iniziativa affinché le persone autorizzate al trattamento, all'interno del Settore/Servizio di competenza di cui è titolare, siano impegnate alla riservatezza e informate sulle modalità di utilizzo dei dati ai fini del rispetto delle prescrizioni del Regolamento generale e delle misure organizzative individuate a tutela della protezione dei dati;
 - h) predisporre, adottare e aggiornare il Registro del trattamento dei dati, nell'ambito di riferimento, ai sensi degli articoli 30 e seguenti del Regolamento generale, secondo le indicazioni fornite dal Responsabile della protezione dei dati personali individuato dal Titolare del trattamento;
 - i) predisporre, di intesa con il DPO, l'analisi dell'impatto (DPIA) laddove sia richiesto, in relazione alla specificità dei processi di lavoro e del trattamento dati personali;
 - j) predisporre, di intesa con il Responsabile della protezione dei dati (DPO) le informative ai cittadini e agli utenti, ogni qualvolta sia richiesto ai fini della comunicazione dei diritti degli interessati alla tutela dei dati personali;
 - k) assicurare l'esercizio del diritto di accesso ai dati degli interessati secondo quanto previsto dall'articolo 15 del Regolamento generale per la protezione dei dati.
3. Il dirigente e gli incaricati di Elevata Qualificazione dei Settori e Servizi dell'Ente, nel caso in cui affidino a un soggetto esterno l'espletamento di servizi che comportino il trattamento dei dati personali per conto dell'ente, è tenuto, ai sensi dell'articolo 2-quaterdecies del d.lgs. 196/2003 a prevedere, nella convenzione o nel contratto che disciplina gli obblighi prestazionali, la definizione delle responsabilità in ordine al trattamento dei dati, designando quale "responsabile del trattamento" i soggetti esterni a cui viene affidato l'incarico e definendone le modalità e gli ambiti di esercizio, secondo le modalità prescritte nel successivo articolo 7.

Articolo 6 – Soggetti autorizzati al trattamento

1. Il Responsabile del trattamento, in ragione dell'articolazione del Settore/Servizio di competenza o per attività che richiedano utilizzo di archivi o banche dati, può designare, con provvedimento formale, degli "autorizzati al trattamento", individuati tra i propri collaboratori, a cui affidare il compito di assicurare tutte le garanzie necessarie per la tutela dei dati personali e per la corrispondente applicazione delle misure previste.
2. Gli autorizzati al trattamento, nelle attività di acquisizione, conservazione, trasmissione ed elaborazione hanno l'obbligo di gestire i dati e le informazioni in modo consapevole nel rispetto delle istruzioni ricevute dal Responsabile del trattamento, nonché delle prescrizioni normative e delle disposizioni adottate dall'ente dall'Autorità garante.
3. E' fatto obbligo a ogni autorizzato al trattamento di assicurare l'integrità dei dati che gli vengono affidati, nonché di garantire il rispetto dei principi di liceità, correttezza, limitazione delle finalità, minimizzazione e di inibirne l'eventuale uso indebito, adottando ogni misura e prescrizioni adottata dall'ente o prescritta dal DPO.
4. In caso di violazione, anche probabile, del trattamento dei dati a lui affidati, ogni autorizzato al trattamento è tenuto a informare tempestivamente il Responsabile del trattamento, fornendo ogni indicazione utile ai fini della valutazione del grado di rischio e l'eventuale adozione della procedura di data breach.
5. Il dirigente e gli incaricati di Elevata Qualificazione dei Settori e Servizi dell'Ente, nell'ambito del settore/servizio di competenza può autorizzare temporaneamente al trattamento di dati personali eventuali soggetti esterni che prestino attività di collaborazione o esercitino attività di studio e ricerca, o altra attività che giustifichi l'accesso alle informazioni del settore/servizio di competenza, nei limiti degli specifici compiti attribuiti.

6. I soggetti autorizzati, ai sensi del comma precedente, utilizzano dati e informazioni nel rispetto delle prescrizioni ricevute avendo cura di garantire l'integrità e la riservatezza di dati personali, informando il Responsabile del trattamento nel caso in cui possano verificarsi incidenti o violazioni in grado di compromettere la sicurezza dei dati personali.
7. I Responsabili del trattamento hanno il compito di riportare l'elenco dei soggetti autorizzati nel registro del trattamento, specificando l'ambito, oltre che le date di inizio e fine dell'autorizzazione.
8. Nel caso di attribuzione ad un dipendente di compiti specifici ulteriori rispetto alle ordinarie mansioni, nonché in caso di assegnazione di un dipendente a gruppi di lavoro intersettoriale, possono essere attribuite specifiche autorizzazioni al trattamento, per il tempo necessario all'espletamento delle nuove mansioni.

Art. 7 Responsabilità dei dipendenti

1. Ogni dipendente, nel momento in cui viene assegnato a un Settore/Servizio, è autorizzato al trattamento dei dati pertinenti ai procedimenti di competenza di quell'ufficio. Conseguentemente, pur in assenza di specifiche autorizzazioni, ma nel limite dei compiti assegnati, ciascun dipendente è autorizzato al trattamento dei dati correlati alle pratiche assegnate o di pertinenza dell'ufficio di appartenenza.
2. I soggetti autorizzati al trattamento utilizzano dati e informazioni nel rispetto delle prescrizioni ricevute avendo cura di garantire l'integrità e la riservatezza di dati personali, informando il Dirigente nel caso in cui possano verificarsi incidenti o violazioni in grado di compromettere la sicurezza dei dati personali
3. I dipendenti debbono astenersi dall'accesso a dati e informazioni che non corrispondano ai compiti formalmente attribuiti e agli ambiti assegnati.
4. Nel caso di utilizzo di sistemi informatici, i dipendenti sono obbligati a rispettare le disposizioni normative e le prescrizioni fornite dall'ente al fine di garantire la sicurezza dei dati e delle comunicazioni.

Art. 8 – I Responsabili esterni del trattamento

1. Laddove l'Ente ricorra all'affidamento a soggetti esterni di servizi che comportino la gestione di dati personali, provvede a individuare il Responsabile esterno del trattamento.
2. L'individuazione del responsabile esterno avviene mediante specifica prescrizione contenuta nel contratto di affidamento, sottoscritta dal dirigente nella qualità di Responsabile interno del trattamento, nel quale siano specificate le tipologie di dati il cui trattamento è affidato all'esterno, le modalità di utilizzo, le garanzie per gli interessati e gli obblighi nei confronti del Titolare.
3. Nel caso in cui si ravvisa la necessità di individuare la responsabilità esterna del trattamento riguardo a un contratto già stipulato, l'Ente potrà provvedere con un atto integrativo o con una comunicazione successiva che definisca gli ambiti e i ruoli delle responsabilità, oltre agli oneri connessi.
4. Il Responsabile esterno del trattamento:
 - a) Ha l'onere di assicurare di avere la capacità strutturale, tecnica ed organizzativa allo scopo di garantire su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
 - b) è tenuto ad adottare le misure tecniche e organizzative adeguate al fine di soddisfare gli obblighi prescritti nel Regolamento europeo 679/2016, oltre alle disposizioni del Garante per il trattamento dei dati personali, nonché le indicazioni fornite dal Responsabile della protezione dei dati individuato dall'Ente.
 - c) Risponde direttamente nel caso in cui alcuna delle violazioni del trattamento sia attribuibile alla gestione dei dati di sua competenza, con particolare riguardo ai casi di indebita distruzione, cancellazione, accesso, modifica o divulgazione dei dati personali trattati.

- d) Assicura di non utilizzare, in nessun caso le informazioni, i dati e i documenti acquisiti dall'Ente o per suo conto, ai fini dell'espletamento del servizio affidato, per finalità diverse da questo.
- e) Garantisce di non consentire la consultazione, la diffusione, la copia o qualsiasi altro trattamento dei dati a soggetti estranei alla propria struttura o diversi da quelli indicati al titolare del trattamento.
- f) Mette a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi specificati ed inoltre acconsente alla effettuazione di eventuali ispezioni per conto del titolare del trattamento.
- g) Si impegna a comunicare al Titolare del trattamento i soggetti che saranno utilizzati nel trattamento dei dati, nella qualità di "operatori del trattamento", dei quali si impegna a garantire riguardo alla riservatezza e adeguatezza.
- h) Si impegna a informare il titolare del trattamento di eventuali modifiche previste al processo di trattamento riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare l'opportunità di opporsi a tali modifiche.
- i) Adotta, se necessario, tutte le misure a garantire il ripristino tempestivo, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico che ne pregiudichi l'accesso o l'utilizzo.
- j) E' tenuto, a conclusione della prestazione, a fornire al titolare del trattamento, ogni dato trattato per suo conto e ad assicurarne, se richiesto, la cancellazione.
- k) Laddove abbia notizie di una violazione del trattamento, anche presunta, è obbligato a informare immediatamente il Titolare del trattamento e il Responsabile della protezione dei dati individuato dall'Ente.
- l) Nel caso in cui sorga la necessità del ricorso ad un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione Europea o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento principale. Quest'ultimo è tenuto a prevedere da parte del responsabile del trattamento che lo supporterà, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente accordo e del regolamento.
- m) Si impegna ad assicurare al Titolare del trattamento l'accesso a qualsiasi informazione, dato o documento relativo al servizio affidato, anche allo scopo di ottemperare agli obblighi previsti dall'art. 15 del Regolamento europeo prima richiamato

Art.9 – Il Responsabile della protezione dati

1. Il Titolare del trattamento individua un professionista esterno a cui affidare l'incarico di Responsabile della protezione dei dati, anche mediante l'affidamento di un servizio a una Società che fornisca assistenza nell'ambito della protezione dei dati personali.

2. Il Responsabile della protezione dei dati, ai sensi dell'articolo 39 del Regolamento UE 2016/679, è incaricato dei seguenti compiti:

- a) informare e fornire consulenza al Titolare e ai Responsabili 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.
- b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e dei Responsabili 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.

- c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento.
 - d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento.
 - e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto 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 è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante.
3. 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.
 4. il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.
 5. 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.
 6. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare o al Responsabile del trattamento.
 7. 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.10 - Sicurezza del trattamento

1. Il Titolare e ciascun Responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto delle caratteristiche del contesto e dei costi di attuazione, nonché della natura, delle finalità del trattamento, della probabilità che il rischio generi danno e della eventuale gravità per i diritti e le libertà delle persone fisiche.
- 2- Le misure tecniche ed organizzative di sicurezza 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- La conformità del trattamento dei dati al RGPD in materia di protezione dei dati personali è dimostrata attraverso l'adozione di idonee misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
- 4- Il Titolare 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.
- 5- I nominativi ed i dati di contatto del Titolare, dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'Ente, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.

Art.11 - Registri delle attività di trattamento

1. Ai sensi dell'art. 30 comma 2 del richiamato Regolamento generale per la protezione dei dati personali, sono istituiti i registri dei **Responsabili interni del trattamento** contenenti:
 - a) il nome e i dati di contatto del responsabile e degli autorizzati al trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
 - b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

- c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
 - d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
 - e) Ogni eventuale informazione che sia prescritta da successive disposizioni normative di legge o dell'Autorità garante della protezione dei dati personali.
2. I registri saranno predisposti mediante strumenti informatici e dovranno essere costantemente aggiornati e riproducibili, quando richiesto, in forma cartacea al fine di assicurarne la conservazione e l'immediata consultazione.
 3. I registri dovranno essere sempre aggiornati e dovranno essere resi disponibili al titolare del trattamento e ostensibili su richiesta del **DPO** o di chiunque abbia diritto all'accesso in base alla normativa vigente.

Art. 12 - 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 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.
2. 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'art. 35, pp. 4-6, RGDP.
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, 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 analogia 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 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.

4. 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.
5. 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 all'Ente.
6. 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.
7. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.
8. 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.

Art. 13 - 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'Ente.
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 dalla violazione 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.
3. 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;
 - decifrazione non autorizzata della pseudonimizzazione;
 - pregiudizio alla reputazione;
 - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
4. 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. I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

- 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 dall’art. 33 RGPD, ed anche la comunicazione all’interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
 6. 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. 14 – Diritti dell’interessato

1. Ogni soggetto interessato, inteso quale persona fisica identificata o identificabile, potrà chiedere l’accesso ai propri dati personali detenuti presso l’ente nonché l’eventuale rettifica o aggiornamento. Potrà inoltre richiedere la cancellazione, laddove risulti un trattamento indebito, errato o ridondante.
2. Nei casi in cui, l’interessato ritenga che il trattamento dei dati non risponda al principio di necessità o sia ingiustificato o conseguenza di un errore, può opporsi segnalando tale abuso al Titolare del trattamento chiedendo l’immediata rettifica del dato o l’adozione delle misure finalizzate ad assicurare il necessario adeguamento.
3. L’Ente è obbligato a fornire a ogni soggetto interessato le informazioni relative al trattamento dei dati personali, nonché agli strumenti di tutela dei propri diritti.