MANUALE SULLA PRIVACY: LINEE GUIDA E MODALITA' OPERATIVE INTERNE PER LA TUTELA E LA PROTEZIONE DEI DATI PERSONALI

A cura del dott. Simone Carmignani
www.carmignaniconsulenza.com

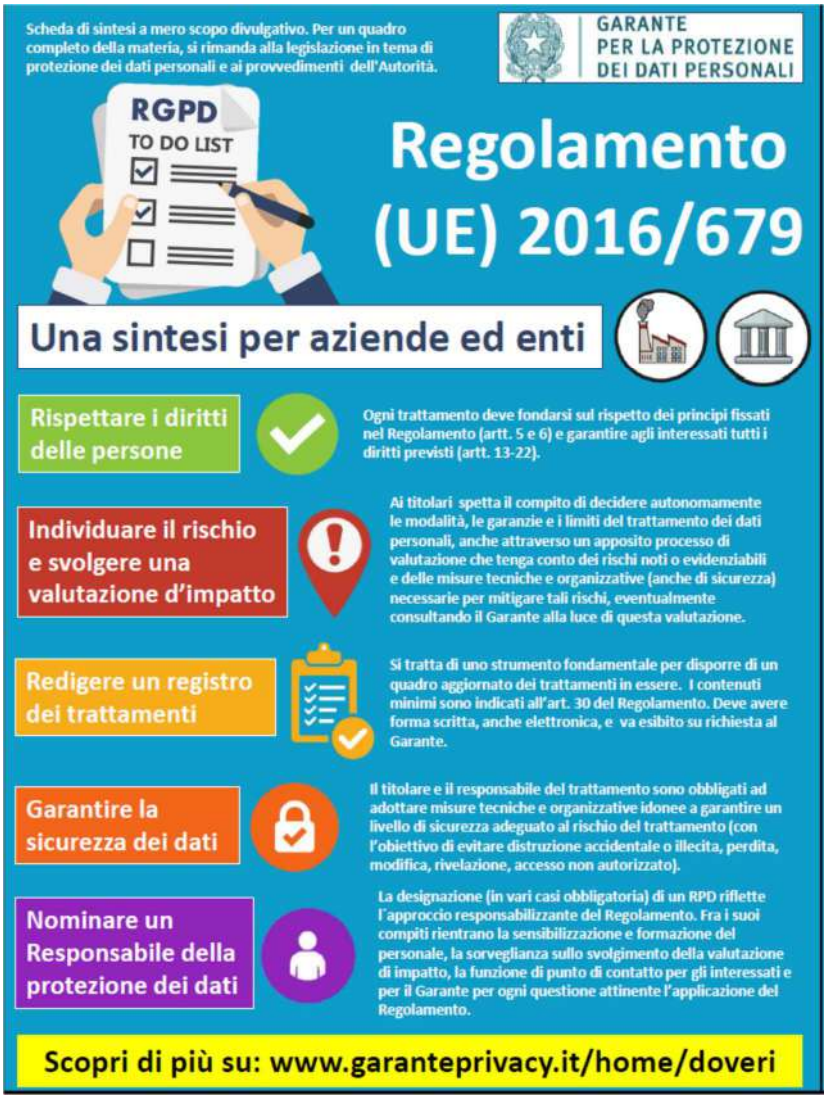
SOMMARIO

1. INTRODUZIONE

Il presente manuale è redatto nell'ambito dell'attività di Responsabile della Protezione dei Dati, è rivolto alle Pubbliche Amministrazioni, alle Società e agli Enti da queste controllati, è finalizzato a definire e raccogliere un insieme di procedure e buone pratiche per la corretta implementazione dei principi della privacy e la tutela dei dati personali sanciti dal GDPR, Regolamento Europeo 679/2016, e dal Codice della Privacy, dlgs 196/2003 così come modificato dal dlgs 101/2018.

Vengono inoltre riprese, riassunte e riportate le più significative linee guida dettate dal Garante per la Protezione dei Dati, dall'Agenzia per l'Italia Digitale e dall'Autorità Anticorruzione, nonché allegati una serie di documenti di lavoro utili per l'implementazione degli obblighi previsti dalla normativa in materia di privacy.

Le procedure illustrate nel manuale non sono vincolanti ma la loro corretta implementazione è fortemente consigliata al fine di rispondere nella maniera più efficace ed efficiente agli obblighi di legge.



2. RIFERIMENTI NORMATIVI

Il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8). Oggi è tutelato, in particolare, dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), oltre che da vari altri atti normativi italiani e internazionali e dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101.

In particolare, il Regolamento (UE) 2016/679 disciplina il trattamento dei dati personali indipendentemente dal fatto che questo sia effettuato o meno nell'Unione europea, sia quando svolto da titolari o responsabili stabiliti in Ue o in un luogo soggetto al diritto di uno Stato membro dell'Ue in virtù del diritto internazionale pubblico (per esempio l'ambasciata o la rappresentanza consolare di uno Stato membro), sia quando il titolare o il responsabile non è stabilito nell'Unione europea ma le attività di trattamento riguardano:

- l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione europea, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
- il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione europea.

Il Regolamento (UE) 2016/679 ha ampliato i diritti riconosciuti all'interessato con riferimento ai dati che lo riguardano, rendendoli maggiormente incisivi in una realtà permeata sempre più dal ricorso alle nuove tecnologie e all'utilizzo della rete.

3. ATTIVITÀ, ORGANIZZAZIONE E SOGGETTI DIRETTAMENTE COINVOLTI

3.1 I DATI PERSONALI

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

Particolarmente importanti sono:

- i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

- i dati rientranti in particolari categorie: si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;

- i dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

3.2 LE PARTI IN GIOCO

Interessato è la persona fisica alla quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale, ecc. di Mario Rossi, questa persona è l'interessato (articolo 4, paragrafo 1, punto 1), del Regolamento UE 2016/679);

Titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento (articolo 4, paragrafo 1, punto 7), del Regolamento UE 2016/679);

Responsabile (esterno) è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati (articolo 4, paragrafo 1, punto 8, del Regolamento UE 2016/679). Il Regolamento medesimo ha

introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. "sub-responsabile" (articolo 28, paragrafo 2).

Il Responsabile può essere individuato quindi all'esterno ogni qual volta un soggetto terzo rispetto l'Amministrazione, che sia una persona fisica o giuridica, tratti dati personali in nome e per conto del Titolare nell'ambito dell'affidamento di un lavoro e di un servizio.

La nomina dei Designati (responsabili interni) a specifici trattamenti dei dati (art. 2 c. quatordecies del dlgs 196/2003) non è obbligatoria ma fortemente consigliata in quanto difficilmente il Titolare ha la possibilità reale di gestire e controllare i singoli trattamenti dei dati, in particolare la nomina dei Designati è sempre consigliata in modo tale da responsabilizzare e coinvolgere nella corretta implementazione dei principi della privacy tutti gli attori che intervengono.

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento;
b) sorvegliare l'osservanza del presente regolamento;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati;
d) cooperare con l'autorità di controllo.

In base all'articolo 37, paragrafo 7, del Regolamento occorre che i soggetti pubblici e privati comunichino al Garante per la protezione dei dati personali il nominativo del Responsabile della Protezione dei dati, se designato, questa disposizione mira a garantire che le autorità di controllo possano contattare il Responsabile della Protezione dei Dati in modo facile e diretto, si ricorda, infatti, che in base all'articolo 39, paragrafo 1, lettera e) del Regolamento, il Responsabile della Protezione dei Dati funge da punto di contatto fra il singolo ente o azienda e il Garante.

Sul sito del Garante è disponibile una procedura online per la comunicazione del nominativo, tale procedura è l'unica che può essere utilizzabile per l'invio dei dati di contatto del Responsabile della protezione dei dati e non potranno essere prese in considerazione le comunicazione effettuate attraverso diversi canali di contatto con il Garante (es. e-mail, posta, ecc.). Attraverso la procedura indicata non è consentito presentare quesiti, richieste e istanze al Garante, in quanto predisposta unicamente per la ricezione delle informazioni relative al Responsabile per la protezione dei dati.

3.3 DIRITTO DI ACCEDERE AI PROPRI DATI PERSONALI

L'interessato ha il diritto di chiedere al titolare del trattamento (soggetto pubblico, impresa, associazione, partito, persona fisica, ecc.) se è in corso o meno un trattamento di dati personali che lo riguardano e, qualora il trattamento sia confermato:

- di ottenere una copia di tali dati;
- di essere informato su:
    - a) le finalità del trattamento;
    - b) le categorie di dati personali trattate;
    - c) i destinatari dei dati;
    - d) il periodo di conservazione dei dati personali;
    - e) quale sia l'origine dei dati personali trattati;
    - f) gli estremi identificativi di chi tratta i dati (titolare, responsabile, rappresentante designato nel territorio dello Stato italiano, destinatari);
    - g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione;
    - h) i diritti previsti dal Regolamento.

Il Regolamento (UE) 2016/679 (articoli da 15 a 22), ha ampliato i diritti riconosciuti all'interessato con riferimento ai dati che lo riguardano, rendendoli maggiormente incisivi nella nostra realtà permeata sempre più dal ricorso alle nuove tecnologie e all'utilizzo della rete. L'interessato può richiedere a chi sta trattando i suoi dati personali che questi siano:

a) rettificati (perché inesatti o non aggiornati), eventualmente integrando informazioni incomplete;

b) cancellati, se:

- i dati non sono più necessari ai fini del perseguimento delle finalità per le quali sono stati raccolti o trattati;
- l'interessato revoca il consenso o si oppone al trattamento; oppure
- i dati sono trattati illecitamente o devono essere cancellati per adempiere a un obbligo legale;
- e se non vi sono altri trattamenti per i quali i dati sono considerati necessari (libertà di espressione e informazione, svolgimento di compiti nel pubblico interesse, trattamenti connessi alla sanità pubblica, ecc.).

c) limitati nel relativo trattamento, se:

- i dati non sono esatti o sono trattati illecitamente e l'interessato si oppone alla loro cancellazione;
- nonostante il titolare non ne abbia più bisogno ai fini del trattamento, i dati sono necessari all'interessato per fare valere un diritto in sede giudiziaria;

d) trasferiti ad un altro titolare (c.d. diritto alla portabilità), se il trattamento si basa sul consenso o su un contratto stipulato con l'interessato e viene effettuato con mezzi automatizzati.

Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare gli interessati, che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

E' possibile poi opporsi al trattamento dei propri dati personali:

a) per motivi connessi alla situazione particolare dell'interessato, da specificare nella richiesta;

b) quando i dati sono trattati per finalità di marketing diretto (senza necessità di motivare l'opposizione).

3.4 TUTELARE I DATI PERSONALI

Ogni persona può tutelare i propri dati personali, in primo luogo, esercitando i diritti previsti dagli articoli da 15 a 22 del Regolamento (UE) 2016/679.

L'interessato può presentare un'istanza al titolare ad esempio mediante lettera raccomandata o pec.

L'istanza può essere riferita, a seconda delle esigenze dell'interessato, a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali che lo riguardano, comunque trattati.

All'istanza il titolare, deve fornire idoneo riscontro, ossia:

- senza ingiustificato ritardo, al più tardi entro 1 mese dal suo ricevimento;
- tale termine può essere prorogato di 2 mesi, qualora si renda necessario tenuto conto della complessità e del numero di richieste. In tal caso, il titolare deve comunque darne comunicazione all'interessato entro 1 mese dal ricevimento della richiesta.

Se si ritiene che il trattamento dei dati che riguardano un interessato non è conforme alla disposizioni vigenti ovvero se la risposta ad un'istanza con cui si esercita uno o più dei diritti previsti dagli articoli 15-22 del Regolamento (UE) 2016/679 non perviene nei tempi indicati o non è soddisfacente, l'interessato può rivolgersi all'autorità giudiziaria o al Garante per la protezione dei dati personali, in quest'ultimo caso mediante un reclamo ai sensi dell'articolo art. 77 del Regolamento (UE) 2016/679.

Il Regolamento europeo non prevede più l'istituto del ricorso per fare valere i diritti di accesso ai dati personali (che pertanto non è più esperibile davanti al Garante a partire dal 25 maggio 2018).

Il reclamo al Garante è un atto circostanziato con il quale si rappresenta una violazione della disciplina rilevante in materia di protezione dei dati personali (articolo 77 del Regolamento UE 679/1996) e artt. da 140-bis a 143 del Codice. Al reclamo segue un'istruttoria preliminare e un eventuale successivo procedimento amministrativo formale, che può portare all'adozione dei provvedimenti di cui all'articolo 58 del Regolamento. Avverso la decisione del Garante è ammesso il ricorso giurisdizionale ai sensi degli articoli 143 e 152 del Codice e dell'articolo 78 del Regolamento, la presentazione del reclamo è gratuita.

Chiunque può rivolgere, ai sensi dell’art. 144 del Codice, una segnalazione, che il Garante può valutare anche ai fini dell'emanazione dei provvedimenti di cui all'art. 58 del Regolamento (indirizzo).

4. PROCESSI DI LAVORO INTERNI E BUONE PRATICHE

4.1 PRINCIPI GENERALI DEL TRATTAMENTO DI DATI PERSONALI

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679, che qui si ricordano brevemente:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Il Regolamento (articolo 5, paragrafo 2) richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è il principio detto di "responsabilizzazione" (o accountability) che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1, del Regolamento, dove si afferma che "il titolare 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."

Il Regolamento, come già previsto dal Codice in materia di protezione dei dati personali, prevede che ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 del Regolamento:

- consenso;
- adempimento obblighi contrattuali;
- interessi vitali della persona interessata o di terzi;
- obblighi di legge cui è soggetto il titolare;
- interesse pubblico o esercizio di pubblici poteri;
- interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Per quanto riguarda le "categorie particolari di dati personali" (articolo 9 del Regolamento), il loro trattamento è vietato, in prima battuta, a meno che il titolare possa dimostrare di soddisfare almeno una delle condizioni fissate all'articolo 9, paragrafo 2 del Regolamento, che qui ricordiamo:

- l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per uno dei seguenti scopi:

- per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
- per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Per alcune di tali finalità sono previste limitazioni o prescrizioni ulteriori, anche nel diritto nazionale.

Quando il trattamento si fonda sul consenso dell'interessato, il titolare deve sempre essere in grado di dimostrare (articolo 7.1 del Regolamento) che l'interessato ha prestato il proprio consenso, che è valido se:

- all'interessato è stata resa l'informazione sul trattamento dei dati personali (articoli 13 o 14 del Regolamento);
- è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse. Il consenso deve essere sempre revocabile.

Occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (articolo 7.2), per esempio all'interno della modulistica, non è ammesso il consenso tacito o presunto (presentando caselle già spuntate su un modulo), quando il trattamento riguarda le "categorie particolari di dati personali" (articolo 9 Regolamento) il consenso deve essere "esplicito", lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – articolo 22), quindi benchè non espressamente previsto qualora il Titolare si trovi nella condizione di dover richiedere il consenso per il trattamento dei dati è necessario che lo faccia nella forma scritta.

Per quanto riguarda l'interesse vitale di un terzo, si può invocare tale base giuridica per il trattamento di dati personali solo se nessuna delle altre condizioni di liceità può trovare applicazione (considerando 46).

Per quanto riguarda l'interesse legittimo prevalente di un titolare o di un terzo, il ricorso a questa base giuridica per il trattamento di dati personali presuppone che il titolare stesso effettui un bilanciamento fra il legittimo interesse suo o del terzo e i diritti e libertà dell'interessato. Dal 25 maggio 2018, dunque, tale bilanciamento non spetta più all'Autorità, in linea di principio. Si tratta di una delle principali espressioni del principio di "responsabilizzazione" introdotto dal Regolamento (UE) 2016/679.

L'interesse legittimo del titolare o del terzo deve risultare prevalente sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità, il Regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti, si ricordi, inoltre, che il legittimo interesse non può essere invocato isolatamente quale base giuridica per il trattamento delle categorie particolari di dati personali (articolo 9, paragrafo 2, del Regolamento).

4.2 TRASPARENZA DEL TRATTAMENTO E L'INFORMATIVA AGLI INTERESSATI

Fatte salve alcune eccezioni, chi intende effettuare un trattamento di dati personali deve fornire all'interessato alcune informazioni anche per metterlo nelle condizioni di esercitare i propri diritti (articoli 15-22 del Regolamento medesimo), l'informativa va sempre resa.

L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del Regolamento) deve essere fornita all'interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati (se raccolti direttamente presso l'interessato: articolo 13 del Regolamento).

Nel caso di dati personali non raccolti direttamente presso l'interessato (articolo 14 del Regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevedeva l'articolo 13, comma 4, del Codice).

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del Regolamento e, in parte, sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.). Se i dati non sono raccolti direttamente presso l'interessato (articolo 14 del Regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.

In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

Il Regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo, se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: articolo 12, paragrafo 1, e considerando 58). Sono

comunque ammessi “altri mezzi”, quindi può essere fornita anche in forma orale, ma nel rispetto delle caratteristiche di cui sopra (articolo 12, paragrafo 1).

In base al Regolamento, si deve porre particolare attenzione alla formulazione dell’informativa, che deve essere soprattutto comprensibile e trasparente per l’interessato, attraverso l’uso di un linguaggio chiaro e semplice. In particolare, bisogna ricordare che per i minori si devono prevedere informative idonee.

4.3 UN APPROCCIO RESPONSABILE AL TRATTAMENTO E IL CONCETTO DI ACCOUNTABILITY

Il Regolamento pone l’accento sulla “responsabilizzazione” di titolari e responsabili, ossia, sull’ adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l’applicazione del Regolamento (artt. 23-25, in particolare, e l’intero Capo IV del Regolamento). Dunque, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Il primo fra tali criteri è sintetizzato dall’espressione inglese “data protection by default and by design” (articolo 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall’inizio le garanzie indispensabili “al fine di soddisfare i requisiti” del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (“sia al momento di determinare i mezzi del trattamento sia all’atto del trattamento stesso”, secondo quanto previsto dall’articolo 25, paragrafo 1, del Regolamento) e richiede, pertanto, un’analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel Regolamento rispetto alla gestione degli obblighi dei titolari: ossia il rischio inerente al trattamento. Quest’ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35- 36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

In conseguenza dell’applicazione del principio di accountability, dal 25 maggio 2018 non sono più previste

- la notifica preventiva dei trattamenti all’autorità di controllo;
- una verifica preliminare da parte del Garante per i trattamenti “a rischio” (anche se potranno esservi alcune eccezioni legate a disposizioni nazionali, previste in particolare dall’articolo 36, paragrafo 5 del Regolamento).

Al loro posto, il Regolamento prevede in capo ai titolari l’obbligo (pressoché generalizzato) di tenere un registro dei trattamenti e, appunto, di effettuare valutazioni di impatto in piena autonomia con eventuale successiva consultazione dell’Autorità.

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti - ma solo se non effettuano trattamenti a rischio (articolo 30, paragrafo 5) - devono tenere un registro delle operazioni di trattamento, i cui contenuti sono indicati all'articolo 30.

Si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. I contenuti del registro sono fissati nell'articolo 30. Tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti, il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

4.4 MISURE DI SICUREZZA

Il titolare del trattamento, come pure il responsabile del trattamento, è obbligato ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato).

Fra tali misure, il Regolamento menziona, in particolare:

- la pseudonimizzazione e la cifratura dei dati;
- misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- misure atte a garantire il tempestivo ripristino della disponibilità dei dati;
- procedure per verificare e valutare regolarmente l'efficacia delle misure di sicurezza adottate.

Per questi motivi, non possono sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza poiché tale valutazione è rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da articolo 32 del Regolamento, vi è, inoltre, la possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate (articolo 32, paragrafo 3).

La protezione dei dati deve inoltre essere garantita mediante l'adozione di opportune misure fisiche di accesso e conservazione degli stessi, nonché di buone pratiche per tutti coloro che trattano i dati personali. Nella pratica questo significa che naturalmente l'accesso ai locali delle strutture dell'Amministrazione deve essere protetto da adeguati sistemi anti intrusione con l'eventuale utilizzo anche di allarmi e videosorveglianza, l'accesso agli uffici deve essere protetto da adeguati sistemi di chiusura come serrature o badge, deve avvenire sempre attraverso previo riconoscimento e deve essere interdetto a coloro che non siano autorizzati in mancanza del personale addetto appartenente all'ufficio in questione che possa vigilare.

Tutti i documenti presenti all'interno degli uffici devono essere sempre correttamente riposti e conservati in maniera che venga garantito l'anonimato dei dati contenuti all'interno di essi, la conservazione dei documenti contenenti in particolare dati sensibili deve prevedere specifici e ulteriori meccanismi di protezione, quali ad esempio casseforti o armadietti dotati di chiave.

L'accesso agli uffici e ai documenti in essi contenuti è di esclusiva competenza del personale appartenente all'ufficio e se previsto dei rispettivi superiori gerarchici, possono accedere altri soggetti se preventivamente autorizzati e regolamentati in modo da definire le procedure per le quali sia garantita sia la responsabilizzazione della protezione dei dati trattati dai dipendenti di un ufficio ma sia al contempo garantito il controllo o la possibilità di intervento qualora ve ne fosse bisogno, è fondamentale che qualsiasi richiesta di accesso ai documenti da parte di non addetti ai lavori, in particolare da soggetti esterni, vada sempre documentata per iscritto e valutata nel rispetto della normativa vigente e dei regolamenti dell'ente.

Tutti i dipendenti e i collaboratori dell'Amministrazione sono responsabilizzati e sono tenuti non solo all'applicazione della normativa vigente ma anche a vigilare e controllare fattivamente il rispetto della protezione dei dati personali, tutto ciò va contemperato e conciliato con la capacità di garantire la continuità dell'erogazione dei pubblici servizi.

5. MISURE MINIME DI SICUREZZA ICT

5.1 Per quanto riguarda la sicurezza informatica ai fini della protezione dei dati personali è possibile fare riferimento alle Misure minime di sicurezza ICT per le Pubbliche Amministrazioni le quali costituiscono parte integrante delle Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni. Questo documento è emesso in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 e costituisce un'anticipazione urgente della regolamentazione completa in corso di emanazione, al fine di fornire alle pubbliche amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

Il raggiungimento di elevati livelli di sicurezza, quando è molto elevata la complessità della struttura e l'eterogeneità dei servizi erogati, può essere eccessivamente oneroso se applicato in modo generalizzato. Pertanto ogni Amministrazione dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi.

I controlli dovrebbero essere implementati per ottenere un determinato livello di sicurezza. Il livello "Minimo" specifica il livello sotto il quale nessuna amministrazione può scendere: i controlli in essa indicati debbono riguardarsi come obbligatori. La seconda, "Standard", può essere assunta come base di riferimento nella maggior parte dei casi, mentre la terza, "Alto", può riguardarsi come un obiettivo a cui tendere.

Di seguito vengono riportate e raccomandazioni del Garante:

www.garanteprivacy.it/flash

1 COME E' FATTA UNA BUONA PASSWORD

Una **buona password**

- deve essere abbastanza **lunga** (almeno 8 caratteri);
- deve contenere **caratteri di almeno 3 diverse tipologie**, da scegliere tra le 4 seguenti: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (punti, trattino, *underscore*, ecc.);
- **non** dovrebbe **contenere riferimenti** personali facili da indovinare (nome, cognome, data di nascita, ecc.);
- **andrebbe periodicamente cambiata**, almeno per i profili più importanti o quelli che usi più spesso (e-mail, *e-banking*, *social network*, ecc.).

Consigli flash

X TUTELARE la tua privacy con buone password

2 UTILIZZA PASSWORD DIVERSE PER ACCOUNT DIVERSI (e-mail, *social network*, ecc.)

In caso di «furto» di una password eviterai così il rischio che anche gli altri profili che ti appartengono possano essere violati.

3 CONSERVA CON CURA LE PASSWORD

- **Non conservare mai** le password su biglietti che poi tieni nel portafoglio o indosso, oppure in *file* non protetti su pc, *smartphone* o *tablet*.
- **Evita di condividere** le password via e-mail, sms, *social network*, *instant messaging*, ecc.. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da pirati informatici.
- Se usi pc, *smartphone* e altri *device* che non ti appartengono, **evita** che possano **conservare in memoria le password da te utilizzate.**

4 PROVA AD USARE SOFTWARE «GESTORI DI PASSWORD»

Si tratta di programmi specializzati che **generano password sicure** e **consentono di appuntare sul pc tutte le password salvandole in un database cifrato sicuro.**
Ce ne sono di vario tipo, gratuiti o a pagamento.

Ti suggeriamo di consultare anche le altre schede informative che trovi su www.garanteprivacy.it/flash e le nostre campagne di comunicazione «Social privacy», «Fatti smart» e «Connetti la testa».
Se hai dubbi e domande, puoi contattare l'URP del Garante: www.garanteprivacy.it/home/urp

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

IL PHISHING: Attenzione ai «pescatori» di dati personali

Il phishing è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente.

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc..

In genere, i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un *form* da compilare. I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

ALCUNI CONSIGLI PER DIFENDERSI

1. IL BUON SENSO PRIMA DI TUTTO

Dati, codici di accesso e password personali non dovrebbero mai essere comunicati a sconosciuti. E' bene ricordare che, in generale, banche, enti pubblici, aziende e grandi catene di vendita non richiedono informazioni personali attraverso e-mail, sms, social media o chat: quindi, meglio evitare di fornire dati personali, soprattutto di tipo bancario, attraverso tali canali. Se si ricevono messaggi sospetti, è bene non cliccare sui link in essi contenuti e non aprire eventuali allegati, che potrebbero contenere virus o programmi *trojan horse* capaci di prendere il controllo di pc e smartphone. Spesso dietro i nomi di siti apparentemente sicuri o le URL abbreviate che si trovano sui social media si nascondono link a contenuti non sicuri. Una piccola accortezza consigliata è quella di posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.

2. OCCHIO AGLI INDIZI

I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti. Tuttavia, capita spesso che contengano anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue. E' utile anche prestare attenzione al mittente (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali). Meglio diffidare dei messaggi con toni intimidatori, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente: possono essere subdole strategie per spingere il destinatario a fornire informazioni personali.

3. PROTEGGERSI MEGLIO

E' utile installare e tenere aggiornato sul pc o sullo smartphone un programma antivirus che protegga anche dal phishing. Programmi e gestori di posta elettronica hanno spesso sistemi di protezione che indirizzano automaticamente nello spam la maggior parte dei messaggi di phishing: è bene controllare che siano attivati e verificarne le impostazioni. Meglio non memorizzare dati personali e codici di accesso nei browser utilizzati per navigare online. In ogni caso, è buona prassi impostare password alfanumeriche complesse, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato: banca online, e-mail, social network, ecc. *[vedi anche la scheda del Garante con i consigli per gestire le password in sicurezza]*, a meno di disporre di sistemi di autenticazione forte (*strong authentication*).

4. ACQUISTI ONLINE IN SICUREZZA

Se si fanno acquisti online, è più prudente usare carte di credito prepagate o altri sistemi di pagamento che permettono di evitare la condivisione di dati del conto bancario o della carta di credito.

5. LA PRUDENZA NON E' MAI TROPPA

Per proteggere conti bancari e carte di credito è bene controllare spesso le movimentazioni e attivare sistemi di *alert* automatico che avvisano l'utente di ogni operazione effettuata. Nel caso si abbia il dubbio di essere stati vittime di phishing è consigliabile contattare direttamente la banca o il gestore della carta di credito attraverso i canali di comunicazione conosciuti e affidabili.

Per segnalazioni e richieste di ulteriori informazioni: urp@gpdp.it

ATTENZIONE AL RANSOMWARE

Il programma che prende «in ostaggio» PC e smartphone

1. COS'E' IL RANSOMWARE?

Il **ransomware** è un programma informatico dannoso che infetta un dispositivo (PC, tablet, smartphone, smart TV), **bloccando l'accesso ai contenuti** (foto, video, file) e **chiedendo un riscatto** *(in inglese, ransom)* per «liberarli». La **richiesta di pagamento** con le relative istruzioni è presentata in una finestra che appare automaticamente sullo schermo del dispositivo infettato. L'utente ha pochi giorni per pagare: **poi il blocco diventa definitivo.** Ci sono **due tipi principali di ransomware**: i **cryptor** (che criptano i file contenuti nel dispositivo rendendoli illeggibili) e i **blocker** (che bloccano l'accesso al dispositivo infettato).

2. COME SI DIFFONDE?

Il ransomware si diffonde soprattutto attraverso **messaggi** - inviati via e-mail, sms o chat o che appaiono su pagine web e social network - che sembrano provenire da **soggetti conosciuti e sicuri** come corrieri espressi, gestori di servizi *(acqua, luce, gas)*, operatori telefonici, soggetti istituzionali, ecc.. Chi li riceve è indotto ingannevolmente ad **aprire allegati** o a **cliccare link o banner** collegati a software dannosi. Il dispositivo infettato può poi «contagiarne» altri, perché il ransomware, impossessandosi della **rubrica dei contatti**, può utilizzarla per **spedire automaticamente messaggi contenenti file dannosi.**

3. COME DIFENDERSI?

La prima difesa è **evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti** *(ad es. un operatore telefonico di cui non si è cliente, un corriere espresso da cui non si aspettano consegne, ecc.)* e **non cliccare su collegamenti a siti sospetti.**
E' utile installare un **antivirus** con estensioni per malware sui propri dispositivi e **mantenere aggiornato il sistema operativo.**
E' fondamentale effettuare **backup periodici dei contenuti**: così, nel caso in cui fosse necessario formattare il dispositivo per sbloccarlo, **i dati in esso contenuti non verranno persi.**

4. COME LIBERARSI DAL RANSOMWARE?

Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di **non ricevere i codici di sblocco**, o addirittura di finire in **liste di «pagatori»** potenzialmente soggetti a periodici attacchi ransomware. L'alternativa è quella di **rivolgersi a tecnici specializzati** capaci di sbloccare il dispositivo. Oppure si può **formattare il dispositivo**, ma con il rischio di perdere tutti i dati in esso contenuti se **non è disponibile un backup.**
E' consigliabile sempre segnalare o denunciare l'attacco ransomware alla Polizia postale, anche per aiutare a prevenire ulteriori truffe.

La scheda ha mere finalità divulgative


www.garanteprivacy.it/flash
1
RISPETTA SEMPRE GLI ALTRI
Chiediti sempre se quello che pubblichi on line può offendere o danneggiare qualcuno. Ricorda che sei responsabile di ciò che scrivi o diffondi su web e social network
Consigli flash
X TUTELARE
la tua privacy
su web e social network
2
Foto, testi e filmati messi in Rete possono restare on line per sempre ed essere visti da chiunque. Ricorda: ciò che pubblichi oggi potrebbe non piacerti più domani, o potrebbe danneggiare la tua reputazione con datori di lavoro, colleghi, compagni di studio, ecc.
RIFLETTI PRIMA DI PUBBLICARE QUALCOSA ON LINE
3
Usa password differenti e complicate per i tuoi account e-mail e per i profili su web e social network e non comunicarle a nessuno. Altrimenti i tuoi dati personali e la tua identità on line potrebbero essere a rischio. Per informazioni, consulta anche la campagna «Connetti la testa» (www.garanteprivacy.it/connettilatesta)
ATTENTO A PIRATI TELEMATICI E LADRI DI IDENTITA' DIGITALE
OCCHIO ALLE TRACCE CHE PUOI LASCIARE ONLINE
5
Puoi verificare le informazioni legate al tuo nome o alla tua attività lavorativa o professionale usando un motore di ricerca. Se lo ritieni necessario, puoi chiedere al sito web di cancellare o rettificare alcuni dati personali che ti riguardano (per informazioni, consulta: www.garanteprivacy.it/home/diritti). Controlla anche i cookie scaricati mentre navighi on line, e ricorda che puoi decidere se dare il consenso a quelli usati a scopo di profilazione (per approfondire, vedi: www.garanteprivacy.it/cookie)
SPAM
4
Leggi sempre con attenzione l'informativa sul trattamento dei dati personali prima di accedere a servizi on line o compilare form sul web. Crea indirizzi e-mail diversi da usare solo per fare acquisti online, accedere a servizi sul web, ricevere newsletter, ecc.. Così la tua posta elettronica personale o lavorativa sarà protetta dal rischio di «contagio spam». Per informazioni, consulta anche la pagina web: www.garanteprivacy.it/spam
PROTEGGITI DALLO SPAM TELEMATICO
Se hai dubbi e domande, puoi contattare l'URP del Garante: www.garanteprivacy.it/home/urp
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

5.2 Di seguito vengono riportate singole schede di controllo contenenti ognuna una famiglia di misure di dettaglio più fine, che possono essere adottate in modo indipendente, consentendo un'ulteriore modulazione utile ad adattare il sistema di sicurezza alla effettiva realtà locale.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X
	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	ID.AM-1		X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	ID.AM-1	X	X	X
		2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	ID.AM-1		X	X
		3	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	ID.AM-1			X

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
1	5	1	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	ID.AM-1			X
	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	ID.AM-1			X

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
2	1	1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco.	ID.AM-2	X	X	X
	2	1	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	ID.AM-2		X	X
		2	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	ID.AM-2		X	X
		3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	ID.AM-2			X
	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ID.AM-2	X	X	X
		2	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	ID.AM-2		X	X
		3	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	ID.AM-2			X
	4	1	Utilizzare macchine virtuali e/o sistemi air-gapped1 per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	ID.AM-2			X

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	PR.IP-1	X	X	X
		2	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	PR.IP-1		X	X
		3	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	PR.IP-2 RC.IM-1			X
	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	PR.IP-1	X	X	X
		2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	PR.IP-2 RC.RP-1	X	X	X
		3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	PR.IP-3		X	X
	3	1	Le immagini d'installazione devono essere memorizzate offline.	PR.IP-2	X	X	X
		2	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	PR.DS-2 PR.IP-2		X	X
	4	1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	PR.AC-3 PR.MA-2	X	X	X

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
3	5	1	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	PR.DS-6		X	X
		2	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	PR.DS-6			X
		3	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	PR.IP-3			X
		4	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	PR.IP-3			X
	6	1	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	PR.IP-3			X
	7	1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	PR.IP-3			X

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
4	1	1	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	ID.RA-1 DE.CM-8	X	X	X
		2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	ID.RA-1 DE.CM-8		X	X
		3	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	DE.CM-8			X
	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	DE.CM-8		X	X
		2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	DE.CM-8		X	X
		3	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	DE.CM-8		X	X
	3	1	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	DE.CM-8		X	X
		2	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	DE.CM-8		X	X
	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	DE.CM-8	X	X	X
		2	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	ID.RA-2		X	X

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
4	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	PR.MA-1	X	X	X
		2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	PR.MA-1	X	X	X
	6	1	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	ID.RA-1 DE.CM-8		X	X
	7	1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	PR.IP-12 RS.MI-3	X	X	X
		2	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	PR.IP-12 RS.MI-3		X	X
	8	1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	ID.RA-4 ID.RA-5 PR-IP.12	X	X	X
		2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	PR.IP-12	X	X	X
	9	1	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	PR.IP-12 RS.MI-3		X	X
	10	1	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	PR.DS-7		X	X

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
5	1	1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	PR.AC-4 PR.PT-3	X	X	X
		2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	PR.AC-4 PR.PT-3	X	X	X
		3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	PR.AC-4 PR.PT-3		X	X
		4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	ID.AM-3 DE.AE-1			X
	2	1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	ID.AM-6 PR.AT-2 DE.CM-3	X	X	X
		2	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	DE.CM-3			X
	3	1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	PR.IP-1	X	X	X
	4	1	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X
		2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X
		3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	ID.AM-6 PR.IP-3		X	X
	5	1	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	PR.PT-1 DE.AE-1 DE.AE-5 DE.CM-1		X	X

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
5	6	1	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	PR.AC-1 PR.AT-2			X
	7	1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	PR.AC-1 PR.AT-2	X	X	X
		2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	PR.AC-1 PR.AT-2		X	X
		3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	PR.AC-1 PR.AT-2	X	X	X
		4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	PR.AC-1	X	X	X
		5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	PR.AC-1		X	X
		6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	PR.AC-1 PR.AT-2		X	X
	8	1	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	PR.AC-1 PR.AT-2 DE.CM-7		X	X
	9	1	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	PR.AT-2 PR.PT-2 PR.PT-3 PR.PT-4		X	X

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
5	10	1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	ID.AM-6	X	X	X
		2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	ID.AM-6	X	X	X
		3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	ID.AM-6 PR.AT-2	X	X	X
		4	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	ID.AM-6 PR.AT-2		X	X
	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	PR.AC-1 PR.AT-2	X	X	X
		2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	PR.AC-1 PR.AC-2	X	X	X

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
8	1	1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	DE.CM-4 DE.CM-5	X	X	X
		2	Installare su tutti i dispositivi firewall ed IPS personali.	DE.CM-1	X	X	X
		3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	DE.AE-3 DE.CM-1 RS.CO-1 RS.MI-1		X	X
	2	1	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	PR.IP-3 DE.DP-1		X	X
		2	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	PR.IP-3 PR.MA-1 PR.MA-2 DE.CM-4		X	X
		3	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	PR.DS-7 DE.CM-4			X
	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	PR.PT-3 DE.CM-7	X	X	X
		2	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	PR.AC-3 DE.AE-1 DE.CM-7			X
	4	1	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	PR.IP-1 RS.MI-1 RS.MI-2		X	X
		2	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	PR.IP-1 RS.MI-1 RS.MI-2			X

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
8	5	1	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	DE.CM-1 DE.CM-4		X	X
		2	Installare sistemi di analisi avanzata del software sospetto.	DE.CM-4			X
	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	DE.CM-1 DE.CM-4		X	X
	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	PR.PT-2	X	X	X
		2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	PR.AT-1 DE.CM-4	X	X	X
		3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	PR.AT-1 DE.CM-4	X	X	X
		4	Disattivare l'anteprima automatica dei contenuti dei file.	PR.AT-1 DE.CM-4	X	X	X
	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	PR.PT-2 DE.CM-4	X	X	X
	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	DE.CM-1 DE.CM-4	X	X	X
		2	Filtrare il contenuto del traffico web.	DE.CM-1 DE.CM-4	X	X	X
		3	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	DE.CM-1 DE.CM-4	X	X	X
	10	1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	DE.CM-1 DE.CM-4		X	X
	11	1	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	ID.AM-6 DE.CM-4 RS.CO-5		X	X

ABSC 10 (CSC 10): COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	PR.IP-4	X	X	X
		2	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	PR.IP-4			X
		3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	PR.IP-4			X
	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	PR.IP-4		X	X
	3	1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	PR.DS-6	X	X	X
	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	PR.AC-2 PR.IP-4 PR.IP-5 PR.IP-9	X	X	X

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

ABSC_ID		#	Descrizione	FNSC	Min.	Std.	Alto
13	1	1	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	ID.AM-5	X	X	X
	2	1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	ID.AM-5 PR.DS-5		X	X
	3	1	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	ID.AM-3 PR.AC-5 PR.DS-1 DE.AE-1			X
	4	1	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	ID.AM-3 DE.CM-1			X
	5	1	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	PR.PT-2			X
		2	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	ID.AM-1 PR.PT-2			X
	6	1	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	ID.AM-3 DE.CM-1			X
		2	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	ID.AM-3 DE.CM-1			X
	7	1	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	ID.AM-3 PR.DS-5 DE.CM-1			X
	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	ID.-AM3 PR.DS-5 DE.CM-1	X	X	X
	9	1	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	PR.AC-4 PR.DS-5			X

6. PRIVACY E TRASPARENZA

6.1 TRASPARENZA E NUOVA DISCIPLINA DELLA TUTELA DEI DATI PERSONALI (REG. UE 2016/679)

A seguito dell'applicazione dal 25 maggio 2018 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)» (si seguito RGPD) e, dell'entrata in vigore, il 19 settembre 2018, del decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali - decreto legislativo 30 giugno 2003, n. 196 – alle disposizioni del Regolamento (UE) 2016/679, sono stati formulati quesiti all'ANAC volti a chiarire la compatibilità della nuova disciplina con gli obblighi di pubblicazione previsti dal d.lgs. 33/2013.

Il regime normativo per il trattamento di dati personali da parte dei soggetti pubblici è, quindi, rimasto sostanzialmente inalterato essendo confermato il principio che esso è consentito unicamente se ammesso da una norma di legge o, nei casi previsti dalla legge, di regolamento. Pertanto, fermo restando il valore riconosciuto alla trasparenza, che concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione (art. 1, d.lgs. 33/2013), occorre che le pubbliche amministrazioni, prima di mettere a disposizione sui propri siti web istituzionali dati e documenti (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, verifichino che la disciplina in materia di trasparenza contenuta nel d.lgs. 33/2013 o in altre normative, anche di settore, preveda l'obbligo di pubblicazione.

Giova rammentare, tuttavia, che l'attività di pubblicazione dei dati sui siti web per finalità di trasparenza, anche se effettuata in presenza di idoneo presupposto normativo, deve avvenire nel rispetto di tutti i principi applicabili al trattamento dei dati personali contenuti all'art. 5 del Regolamento (UE) 2016/679, quali quelli di liceità, correttezza e trasparenza; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza tenendo anche conto del principio di "responsabilizzazione" del titolare del trattamento. In particolare, assumono rilievo i principi di adeguatezza, pertinenza e limitazione a quanto necessario rispetto alle finalità per le quali i dati personali sono trattati («minimizzazione dei dati») (par. 1, lett. c) e quelli di esattezza e aggiornamento dei dati, con il conseguente dovere di adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (par. 1, lett. d).

Il medesimo d.lgs. 33/2013 all'art. 7 bis, co. 4, dispone inoltre che «Nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione». Si richiama anche quanto previsto all'art. 6 del d.lgs. 33/2013 rubricato "Qualità delle informazioni" che risponde alla esigenza di assicurare esattezza, completezza, aggiornamento e adeguatezza dei dati pubblicati. In generale, in relazione alle cautele da adottare per il rispetto della normativa in materia di protezione

dei dati personali nell'attività di pubblicazione sui siti istituzionali per finalità di trasparenza e pubblicità dell'azione amministrativa, si rinvia alle più specifiche indicazioni fornite dal Garante per la protezione dei dati personali.

Si ricorda inoltre che, in ogni caso, ai sensi della normativa europea, il Responsabile della Protezione dei Dati-RPD (vedi infra paragrafo successivo) svolge specifici compiti, anche di supporto, per tutta l'amministrazione essendo chiamato a informare, fornire consulenza e sorvegliare in relazione al rispetto degli obblighi derivanti della normativa in materia di protezione dei dati personali (art. 39 del RGPD).

6.2 RAPPORTI TRA RPCT E RESPONSABILE DELLA PROTEZIONE DEI DATI –RPD

Un indirizzo interpretativo con riguardo ai rapporti fra il Responsabile della prevenzione della corruzione (RPCT) e il Responsabile della protezione dei dati - RPD, figura introdotta dal Regolamento (UE) 2016/679 (artt. 37-39), è stato sollecitato all'Autorità da diverse amministrazioni. Ciò in ragione della circostanza che molte amministrazioni e soggetti privati tenuti al rispetto delle disposizioni contenute nella l. 190/2012, e quindi alla nomina del RPCT, sono chiamate a individuare anche il RPD.

Come chiarito dal Garante per la protezione dei dati personali l'obbligo investe, infatti, tutti i soggetti pubblici, ad esempio, le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.

Secondo le previsioni normative, il RPCT è scelto fra personale interno alle amministrazioni o enti (si rinvia al riguardo all'art. 1, co. 7, della l. 190/2012 e alle precisazioni contenute nei Piani nazionali anticorruzione 2015 e 2016). Diversamente il RPD può essere individuato in una professionalità interna all'ente o assolvere ai suoi compiti in base ad un contratto di servizi stipulato con persona fisica o giuridica esterna all'ente (art. 37 del Regolamento (UE) 2016/679).

Fermo restando, quindi, che il RPCT è sempre un soggetto interno, qualora il RPD sia individuato anch'esso fra soggetti interni, l'Autorità ritiene che, per quanto possibile, tale figura non debba coincidere con il RPCT. Si valuta, infatti, che la sovrapposizione dei due ruoli possa rischiare di limitare l'effettività dello svolgimento delle attività riconducibili alle due diverse funzioni, tenuto conto dei numerosi compiti e responsabilità che la normativa attribuisce sia al RPD che al RPCT.

Eventuali eccezioni possono essere ammesse solo in enti di piccoli dimensioni qualora la carenza di personale renda, da un punto di vista organizzativo, non possibile tenere distinte le due funzioni. In tali casi, le amministrazioni e gli enti, con motivata e specifica determinazione, possono attribuire allo stesso soggetto il ruolo di RPCT e RPD. Giova sottolineare che il medesimo orientamento è stato espresso dal Garante per la protezione dei dati personali nella FAQ n. 7 relativa al RPD in ambito pubblico, laddove ha chiarito che «In linea di principio, è quindi ragionevole che negli enti pubblici di grandi dimensioni, con trattamenti di dati personali di particolare complessità e sensibilità, non vengano assegnate al RPD ulteriori responsabilità (si pensi, ad esempio, alle amministrazioni centrali, alle agenzie, agli istituti previdenziali, nonché alle regioni e alle asl). In tale quadro, ad esempio, avuto riguardo, caso per caso, alla specifica struttura organizzativa, alla dimensione e alle

attività del singolo titolare o responsabile, l'attribuzione delle funzioni di RPD al responsabile per la prevenzione della corruzione e per la trasparenza, considerata la molteplicità degli adempimenti che incombono su tale figura, potrebbe rischiare di creare un cumulo di impegni tali da incidere negativamente sull'effettività dello svolgimento dei compiti che il RGPD attribuisce al RPD».

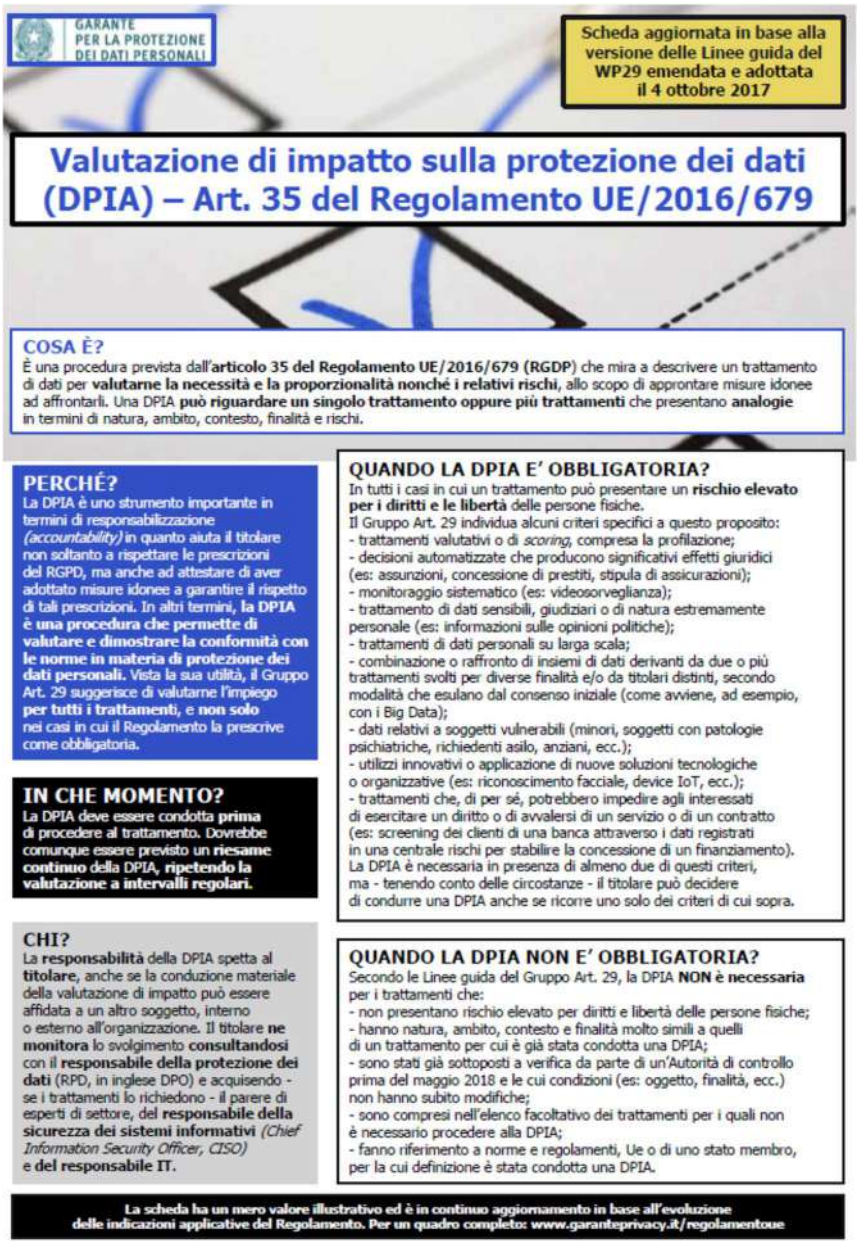
Resta fermo che, per le questioni di carattere generale riguardanti la protezione dei dati personali, il RPD costituisce una figura di riferimento anche per il RPCT, anche se naturalmente non può sostituirsi ad esso nell'esercizio delle funzioni. Si consideri, ad esempio, il caso delle istanze di riesame di decisioni sull'accesso civico generalizzato che, per quanto possano riguardare profili attinenti alla protezione dei dati personali, sono decise dal RPCT con richiesta di parere al Garante per la protezione dei dati personali ai sensi dell'art. 5, co. 7, del d.lgs. 33/2013. In questi casi il RPCT ben si può avvalere, se ritenuto necessario, del supporto del RDP nell'ambito di un rapporto di collaborazione interna fra gli uffici ma limitatamente a profili di carattere generale, tenuto conto che proprio la legge attribuisce al RPCT il potere di richiedere un parere al Garante per la protezione dei dati personali. Ciò anche se il RPD sia stato eventualmente già consultato in prima istanza dall'ufficio che ha riscontrato l'accesso civico oggetto del riesame.

Le considerazioni sopra espresse per le amministrazioni e gli enti valgono anche per i soggetti di cui all'art. 2-bis, co. 2, del d.lgs. 33/2013 tenuti a nominare il RPCT, qualora, ai sensi del Regolamento (UE) 2016/679, siano obbligati a designare anche il RPD. Ci si riferisce agli enti pubblici economici, agli ordini professionali, alle società in controllo pubblico come definite all'art. 2, co. 1, lett. m), del d.lgs. 175 del 2016, alle associazioni, alle fondazioni e agli enti di diritto privato comunque denominati, anche privi di personalità giuridica, con bilancio superiore a cinquecentomila euro, la cui attività sia finanziata in modo maggioritario per almeno due esercizi finanziari consecutivi nell'ultimo triennio da pubbliche amministrazioni e in cui la totalità dei titolari o dei componenti dell'organo d'amministrazione o di indirizzo sia designata da pubbliche amministrazioni (Cfr. determinazione ANAC 1134/2017).

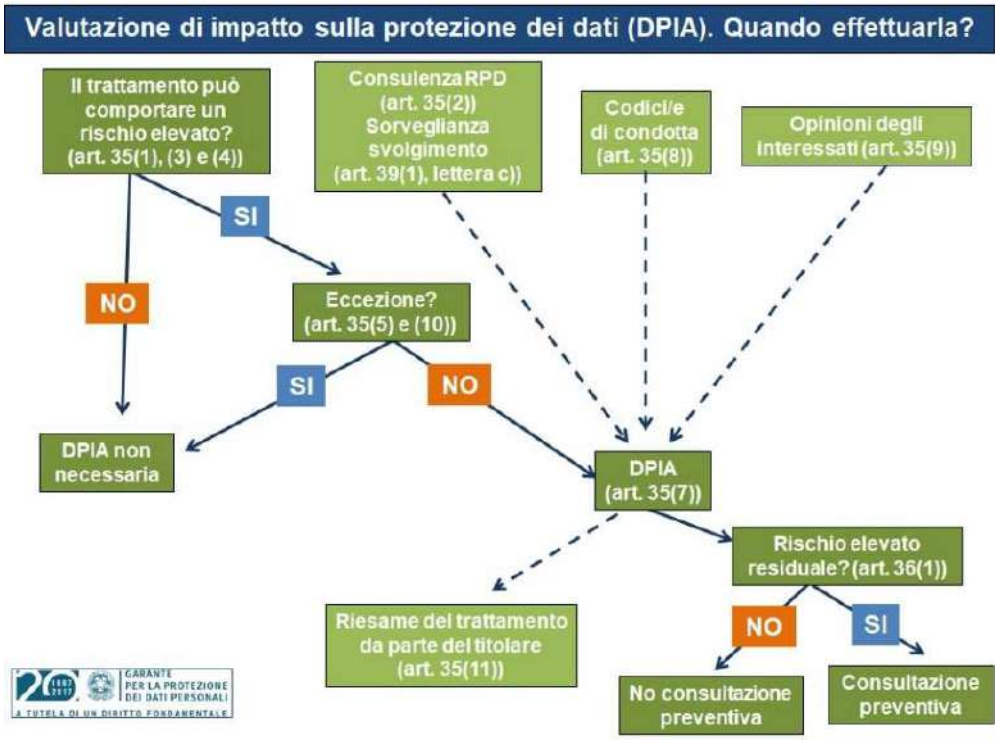
7. VALUTAZIONE DELL'IMPATTO SULLA PROTEZIONE DEI DATI

7.1 QUANDO EFFETTUARE UNA VALUTAZIONE D'IMPATTO

Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.



Le Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" hanno individuato i seguenti nove criteri da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un "rischio elevato".



Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "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".
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito

telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Il ricorrere di due o più dei predetti criteri è indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati e per il quale è quindi richiesta una valutazione d'impatto sulla protezione dei dati, ad ogni modo "quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali", tale elenco è riferito esclusivamente a

tipologie di trattamento soggette al meccanismo di coerenza e che non è esaustivo, restando fermo quindi l'obbligo di adottare una valutazione d'impatto sulla protezione dei dati laddove ricorrano due o più dei criteri individuati dal WP 248, rev. 01 e che in taluni casi "un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno dei predetti criteri richieda una valutazione d'impatto sulla protezione dei dati".

Il messaggio finale delle linee-guida (già sottoposte a consultazione pubblica) è che la valutazione di impatto costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri. In questo senso, la valutazione di impatto permette di realizzare concretamente l´altro fondamentale principio fissato nel regolamento 2016/679, ossia la protezione dei dati fin dalla fase di progettazione (data protection by design) di qualsiasi trattamento.

7.2 UN SOFTWARE PER LA VALUTAZIONE DI IMPATTO

La CNIL, l´Autorità francese per la protezione dei dati, ha messo a disposizione un software di ausilio ai titolari in vista della effettuazione della valutazione d´impatto sulla protezione dei dati (DPIA).

Il software qui presentato NON costituisce un modello al quale fare riferimento in ogni situazione di trattamento, essendo stato concepito soprattutto come ausilio metodologico per le PMI. Offre in ogni caso un focus sugli elementi principali di cui si compone la procedura di valutazione d´impatto sulla protezione dei dati. Potrebbe costituire quindi un utile supporto di orientamento allo svolgimento di una DPIA, ma non va inteso come schema predefinito per ogni valutazione d´impatto che va integrata in ragione delle tipologie di trattamento esaminate.

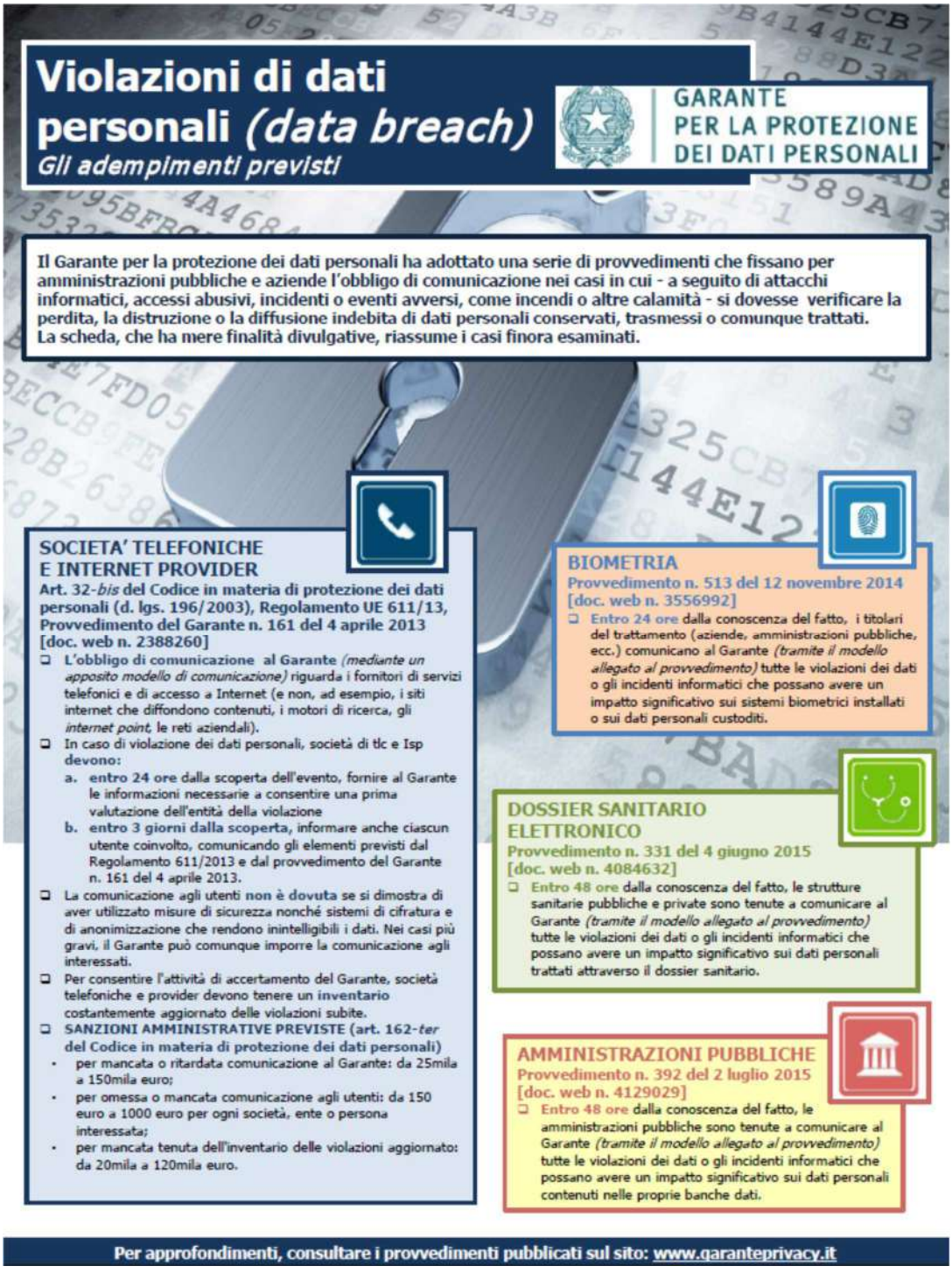
E´ inoltre bene ricordare che la valutazione d´impatto sulla protezione dei dati deve tenere conto del rischio complessivo che il trattamento previsto può comportare per i diritti e le libertà degli interessati, alla luce dello specifico contesto. Pertanto, il concetto di rischio non si esaurisce nella considerazione delle possibili violazioni o minacce della sicurezza dei dati.

8. DATA BREACH

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

Per questa ragione, anche sulla base della normativa europea, il Garante per la protezione dei dati personali ha adottato negli ultimi anni una serie di provvedimenti che introducono in determinati settori l´obbligo di comunicare eventuali violazioni di dati personali (DATA BREACH) all´Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

I casi e gli adempimenti previsti dai provvedimenti del Garante (doc. web nn. 2388260, 3556992, 4084632 e 4129029) sono riassunti in una infografica che offre un prospetto sintetico sulla materia, si ricorda poi che le notifiche al Garante per possibili data breach vanno effettuate entro 72 ore dall'apprendimento o ricevimento della notizia e occorre utilizzare il modello disponibile sul suo sito web.


Violazioni di dati personali (data breach)
Gli adempimenti previsti
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
Il Garante per la protezione dei dati personali ha adottato una serie di provvedimenti che fissano per amministrazioni pubbliche e aziende l'obbligo di comunicazione nei casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o comunque trattati. La scheda, che ha mere finalità divulgative, riassume i casi finora esaminati.
SOCIETA' TELEFONICHE E INTERNET PROVIDER
Art. 32-bis del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]
L'obbligo di comunicazione al Garante (mediante un apposito modello di comunicazione) riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli internet point, le reti aziendali).
In caso di violazione dei dati personali, società di tlc e Isp devono:
a. entro 24 ore dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione
b. entro 3 giorni dalla scoperta, informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013.
La comunicazione agli utenti non è dovuta se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un inventario costantemente aggiornato delle violazioni subite.
SANZIONI AMMINISTRATIVE PREVISTE (art. 162-ter del Codice in materia di protezione dei dati personali)
per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
per omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.
BIOMETRIA
Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992]
Entro 24 ore dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.
DOSSIER SANITARIO ELETTRONICO
Provvedimento n. 331 del 4 giugno 2015 [doc. web n. 4084632]
Entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.
AMMINISTRAZIONI PUBBLICHE
Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]
Entro 48 ore dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.
Per approfondimenti, consultare i provvedimenti pubblicati sul sito: www.garanteprivacy.it

9.FONTI

Fonti ufficiali e autorevoli da cui sono state liberamente tratte e riportate alcune informazioni contenute nel presente Manuale:

- GDPR, Regolamento Europeo 679/2016
- Codice sulla Privacy, dlgs 196/2003
- Aggiornamento al Codice della Privacy, dlgs 101/2018
- WWW.GARANTEPRIVACY.IT
- WWW.ANTICORRUZIONE.IT
- WWW.AGID.GOV.IT
- WWW.CNIL.FR

10. ALLEGATI

Si allegano al presente Manuale alcuni documenti di lavoro ed esempi ai fini della corretta implementazione della privacy:

a. Bozza di Regolamento di Ente sulla protezione dei dati personali
b. Bozza di Regolamento sulla videosorveglianza
c. Bozza di convenzione con le forze dell'ordine per l'utilizzo della videosorveglianza
d. Registri del trattamento dei dati
e. Nomina del responsabile della protezione dati
f. Nomina dei designati a specifici trattamenti dati
g. Nomina dei responsabili del trattamento dati
h. Informativa estesa sulla privacy
i. Riferimento all'informativa sulla privacy per i documenti
j. Riferimento all'informativa sulla privacy per l'email
k. Valutazione d'impatto sulla protezione dei dati

COMUNE DI _____

PROVINCIA DI _____

Regolamento per l'applicazione del RGPD (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e del Codice Nazionale sulla Privacy dlgs 196/2003

Approvato con Delibera di Consiglio Comunale n. ___ del _____

Sommario

Art. 1 - Oggetto del Regolamento

1. Il presente Regolamento disciplina le misure organizzative e le regole di dettaglio per la efficace attuazione da parte del Comune di _____ del "General Data Protection Regulation (EU) 2016/679" (RGPD) ovvero "Regolamento generale sulla protezione dei dati" n. 679 del 27 aprile 2016 (di seguito indicato come RGPD), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali nonché alla libera circolazione di tali dati.

Art. 2 – Quadro normativo di riferimento

1. Il presente Regolamento tiene conto del seguente quadro normativo di riferimento:
   a) Codice in materia di dati personali (D.Lgs. n. 196/2003);
   b) Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.Lgs. n.196 del 30 giugno 2003);
   c) Linee guida e raccomandazioni del Garante;
   d) RGPD del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
   e) Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del RGPD (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
   f) D.Lgs. n. 101/2018 di adeguamento della normativa interna al RGPD;
   g) Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) – 14/EN;
   h) Linee-guida sui responsabili della protezione dei dati (RPD) – WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
   i) Linee-guida sul diritto alla "portabilità dei dati" – WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
   j) Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico Titolare o Responsabile del trattamento – WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
   k) Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 – WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
   l) Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative – WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;

m) Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione – WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
n) Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) – WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
o) Parere del WP29 sulla limitazione della finalità – 13/EN WP 203;
p) Norme internazionali;
q) Regolamenti interni dell'Ente.

Art. 3 – Definizioni

1. Il presente regolamento si avvale delle seguenti definizioni:
   - "Codice": D.Lgs. n. 196/2003;
   - "RGPD": Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016;
   - "Regolamento": il presente Regolamento;
   - "Titolare": il Comune di _____ che adotta il presente Regolamento, con sede in _____ ;
   - "I designate al trattamento dei dati" (responsabili interni): i dirigenti oppure i responsabili titolari di posizione organizzativa delle strutture di massima dimensione in cui si articola l'organizzazione dell'Ente, designati dal Sindaco per l'esercizio di compiti e poteri in materia di trattamento dei dati personali.
2. Il presente regolamento recepisce le definizioni del D.Lgs. n. 196/2003 e del RGPD, fermo restando che, in caso di discordanza, prevalgono le definizioni contenute nei rispettivi testi normativi.

Art. 4–Finalità

1. Il Comune di _____, nell'assolvimento delle proprie finalità istituzionali secondo i principi di trasparenza, efficacia ed economicità, garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.
2. Ai fini del presente Regolamento, per finalità istituzionali del Comune si intendono le funzioni ad esso attribuite dalle leggi, dallo statuto e dai regolamenti o per effetto di accordi e/o convenzioni.
3. I trattamenti di dati personali sono compiuti dal Comune per le seguenti finalità:
   a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:

- l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
- la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è in questo caso stabilita dalla fonte normativa che lo disciplina;
c) l'esecuzione di un contratto con i soggetti interessati;
d) le specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

4. In applicazione di quanto disposto dall'art. 25 del RGPD, i trattamenti di dati personali all'interno dell'Ente devono sottostare ai seguenti principi:
   - sin dall'inizio di una nuova tipologia di trattamento (fase di progettazione) la scelta delle modalità e dei mezzi utilizzati deve basarsi sulla necessità del rispetto della riservatezza e dei diritti fondamentali degli interessati ("privacy by design");
   - l'impostazione e l'organizzazione dei processi lavorativi deve costantemente sottostare a detta necessità, al fine di trattare, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento ("privacy by default").
5. In adempimento dell'obbligo di comunicazione interna ed esterna, del rispetto degli obblighi di trasparenza e di semplificazione dell'azione amministrativa, il Comune favorisce la trasmissione di dati e documenti tra le banche dati e gli archivi del Comune stesso, degli enti territoriali, degli enti pubblici, dei gestori e degli incaricati di pubblico servizio, operanti nell'ambito dell'Unione Europea, nell'ambito di specifiche disposizioni di legge o protocolli d'intesa.
6. La trasmissione dei dati può avvenire anche attraverso l'utilizzo di sistemi informatici e telematici, reti civiche e reti di trasmissione di dati ad alta velocità.
7. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi ed i procedimenti amministrativi di competenza del Titolare effettuati per lo svolgimento delle finalità istituzionali del medesimo, vanno gestiti conformemente alle disposizioni del Codice, del RGPD, del presente Regolamento e delle Linee Guida e dei provvedimenti del Garante.

Art. 5 – Principi e responsabilizzazione

1. Vengono integralmente recepiti, nell'ordinamento interno del Comune di _____, i principi del RGPD, per effetto dei quali i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, paragrafo 1 del RGPD, considerato incompatibile con le finalità iniziali ("limitazione della finalità");
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati in base al principio di "minimizzazione dei dati";
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati in base al principio di "esattezza";
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati in base al principio di "limitazione della conservazione"; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dallo stesso regolamento a tutela dei diritti e delle libertà dell'interessato;
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali in base ai principi di "integrità e riservatezza";
g) configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità (principio di "necessità").

2. Il Titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di comprovarlo in base al principio di "responsabilizzazione".

Art. 6 – Liceità del trattamento

1. Vengono integralmente recepiti, nell'ordinamento interno del Titolare, le disposizioni del RGPD in odine alla liceità del trattamento e, per l'effetto, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
    a. l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
    b. il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c. il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
d. il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e. il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
f. il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

2. La lettera f) di cui al comma precedente non si applica al trattamento di dati effettuato dal Titolare nell'esecuzione dei propri compiti e funzioni. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1 del RGPD, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il Titolare tiene conto, tra l'altro:
   - di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
   - del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
   - della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del RGPD, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del medesimo RGPD;
   - delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
   - dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Art. 7 – Informativa

1. Il Titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste dal RGPD e dall'art 13 del Codice, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
2. L'informativa è data per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online.
3. L'informativa è fornita, mediante idonei strumenti:
   a) Pubblicazione sul sito web dell'ente dell'informativa estesa, nella quale sono indicati anche i soggetti a cui l'utente può rivolgersi per ottenere

maggiori informazioni ed esercitare i propri diritti e le indicazioni sull'utilizzo dei cookie;
b) attraverso appositi moduli da consegnare agli interessati;
c) avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del Titolare, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del Titolare;
d) apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il Titolare.

4. L'informativa da fornire agli interessati può essere fornita anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.
5. Il Titolare garantisce all'interessato:
   a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
6. Nel fornire l'informativa, il Titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

Art. 8–Consenso dell'interessato

1. Il Titolare non deve richiedere agli interessati il consenso per il trattamento dei loro dati personali allorquando il trattamento dei dati è effettuato nello svolgimento dei propri compiti istituzionali di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito dal diritto dell'Unione o dello Stato.
2. Nelle fattispecie diverse da quelle di cui al precedente comma 1, qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
3. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
4. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prestato prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

Art. 9 – Sensibilizzazione e formazione

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati e migliorare la qualità del servizio.
2. A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale del Titolare e l'attività informativa diretta a tutti coloro che hanno rapporti con il Titolare.
3. Il dipendente si impegna ad acquisire copia del Regolamento, prenderne visione ed attenersi alle sue prescrizioni.
4. Il Titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, anche integrati con gli interventi di formazione anticorruzione, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.
5. La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene altresì integrata e coordinata con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il Titolare.

Art. 10 – Trattamento dei dati personali, ricognizione dei trattamenti e indice dei trattamenti

1. Le disposizioni del presente Regolamento si intendono riferite al trattamento, alla diffusione e alla comunicazione dei dati all'esterno.
2. Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del Titolare, solo da parte dei soggetti appositamente autorizzati:

   - Titolare;
   - Designati al trattamento dei dati (dirigenti oppure responsabili delle strutture di massima dimensione in cui è articolata l'organizzazione del Comune);
   - Dipendenti, professionisti, collaboratori esterni e società fornitrici autorizzati al trattamento dei dati.
3. Non è consentito il trattamento da parte di persone non autorizzate.
4. L'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Ente, comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale il Comune provvede alla organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitare l'accesso e la fruizione, anche presso le strutture dipendenti.

5. Ogni richiesta di accesso ai dati personali da parte delle strutture e dei dipendenti comunali deve essere soddisfatta nella misura necessaria al perseguimento dell'interesse istituzionale.
6. Il Titolare e tutti i soggetti coinvolti nel trattamento dei dati si attengono alle modalità di trattamento indicate nel Codice, nel RGPD, nonché nelle disposizioni attuative e nelle Linee guida del Garante per la protezione dei dati personali.

Art. 11 – Trattamento di categorie particolari di dati (così detti dati sensibili)

1. È vietato trattare, secondo quanto previsto dall'art. 9 del RGPD, dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
2. Il divieto di cui al precedente comma non si applica se si verifica uno dei seguenti casi:

   a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al comma 1;

   b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

   c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

   d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

   e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

   f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al successivo comma 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, del RGPD sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al comma 1 possono essere trattati per le finalità di cui al comma 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o dello Stato o alle norme stabilite dagli organismi nazionali competenti.

Art.12 – Trattamento dei dati sensibili e giudiziari

1. Il Titolare conforma il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.
2. A tale fine, il Titolare applica i principi degli articoli 20, 21 e 22 del Codice per il trattamento di dati sensibili e giudiziari, nonché le pertinenti disposizioni del RGPD, e si conforma alle Linee Guida del Garante in materia.
3. Il Titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati sensibili e giudiziari.

Art.13 - Trattamento dei dati sensibili relativi alla salute

1. Il Titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali sensibili relativi allo stato di salute.
2. I dati idonei a rivelare lo stato di salute e la vita sessuale sono trattati da soggetti adeguatamente formati e sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.

Art. - 14 Trattamento dei dati del personale

1. Il Titolare tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo.
2. Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico o economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, relativamente al personale in servizio o in quiescenza.
3. Secondo la normativa vigente, il Titolare adotta le massime cautele nel trattamento di informazioni personali del proprio personale dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose filosofiche o d'altro genere e l'origine razziale ed etnica.
4. Il trattamento dei dati sensibili del dipendente, da parte del datore di lavoro, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati personali e, quando non si possa prescindere dall'utilizzo dei dati giudiziari e sensibili, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.
5. La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando diciture generiche o codici numerici.
6. Non sono infatti ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di natura sensibile.
7. Il Titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

Art. 15 - Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali

1. I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico, anche per ciò che concerne i tipi di dati sensibili e giudiziari, e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.
2. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.
3. Il Titolare si conforma alle Linee guida del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.

Art. 16 – Diritti dell'interessato

1. Il Titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti dell'interessato, in conformità alla disciplina contenuta nel RGPD e nel Codice.

Art. 17 – Diritto di accesso

1. Il presente Regolamento tiene conto della disciplina del RGPD in tema di diritto di accesso secondo la quale l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

    a) le finalità del trattamento;
    b) le categorie di dati personali in questione;
    c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di Paesi terzi o organizzazioni internazionali;
    d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
    e) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
    f) il diritto di proporre reclamo a un'autorità di controllo;
    g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
    h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del RGPD, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate.
3. Il Titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il Titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi necessari. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
4. Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Art. 18 – Diritto alla rettifica e cancellazione

1. Il presente Regolamento tiene conto della disciplina del RGPD in tema di diritto di rettifica e cancellazione («diritto all'oblio»), di seguito indicata.
2. Quanto al diritto di rettifica, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
3. Il Titolare comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
4. Quanto al diritto "all'oblio", consistente nel diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, lo stesso non si applica nella misura in cui il trattamento sia necessario:
   a) per l'esercizio del diritto alla libertà di espressione e di informazione;
   b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
   c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 del RGPD;
   d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 del RGPD, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
   e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 19 – Diritto alla limitazione

1. Il presente Regolamento tiene conto della disciplina del RGPD in tema di diritto alla limitazione di seguito indicata.
2. L'interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle seguenti condizioni:
   a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare per verificare l'esattezza di tali dati personali;
   b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
   c) benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del RGPD, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.
3. Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18 del RGPD, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
4. L'interessato che ha ottenuto la limitazione del trattamento a norma del comma 1 è informato dal Titolare prima che detta limitazione sia revocata.
5. Il Titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
6. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Art. 20 – Diritto alla portabilità

1. Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del RGPD, il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Art. 21 – Diritto di opposizione e processo decisionale automatizzato relativo alle persone

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del RGPD, compresa la profilazione sulla base di tali disposizioni. Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali per motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi,

sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Il diritto di cui ai paragrafi 1 e 2 dell'art. 21 del RGPD è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
3. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
4. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 del RGPD, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Art.22 – Modalità di esercizio dei diritti dell'interessato

1. Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del RGPD, del Codice e del presente Regolamento.
2. La richiesta per l'esercizio dei diritti può essere fatta pervenire:
    a) direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso, come ad esempio, la conoscenza personale;
    b) tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;
    c) tramite chi esercita la potestà o la tutela, per i minori e gli incapaci;
    d) in caso di persone decedute, da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;
    e) dalla persona fisica legittimata in base ai relativi statuti od ordinamenti, se l'interessato è una persona giuridica, un ente o un'associazione.
3. La richiesta, per l'esercizio dei diritti di accesso ai dati personali, può essere esercitata dall'interessato solo in riferimento alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.
4. L'istanza è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
5. Il soggetto competente alla valutazione dell'istanza è il Designato, ossia il dirigente/responsabile in posizione apicale competente per materia, il quale

decide sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati.

6. All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa.
7. I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo.
8. Il Titolare è tenuto a conformarsi alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.

Art. 23 - Titolare del trattamento

1. Il Comune di _____, rappresentato ai fini previsti dal RGPD dal Sindaco pro-tempore, è l'autorità pubblica Titolare del trattamento dei dati ai sensi del RGPD ed esercita le proprie prerogative, poteri e doveri in ordine alle finalità ed ai mezzi del trattamento dei dati personali procedendo alla designazione e nomina: a) degli organismi/soggetti previsti dalla normativa e rimessi alla determinazione del Titolare nonché b) di eventuali gruppi di lavoro e/o team di progetto a supporto di specifiche attività.
2. 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, il Titolare definisce gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento ed è tenuto a mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali viene effettuato in modo conforme a quanto previsto dal RGPD.
3. Il Titolare definisce le misure fin dalla fase di progettazione e le mette in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
4. Nel caso in cui un tipo di trattamento, in particolare allorché questo prevede 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": Data Protection Impact Assessment) ai sensi dell'art. 35 del RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 35.
5. Il Titolare provvede inoltre:
    - a nominare, con proprio atto, nelle persone del Segretario comunale e dei responsabili delle singole strutture di massima dimensione in cui si articola l'organizzazione comunale (dirigenti o, in mancanza, responsabili titolari di posizione organizzativa), i Designati al trattamento (Responsabili interni), ai quali sono attribuiti compiti, funzioni e poteri in ordine ai processi, procedimenti e adempimenti relativi al trattamento dei dati personali contenuti nelle banche dati esistenti nelle articolazioni

organizzative di competenza di ciascun Referente, alla sicurezza e alla formazione, impartendo ad essi le necessarie istruzioni in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;

- a nominare il Responsabile della protezione dei dati (RPD);
- a nominare i Responsabili (esterni) del trattamento;
- a pubblicare ed aggiornare, sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente, i propri dati di contatto e quelli del Responsabile della protezione dati;
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
- ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.
- Tenere il registro unico dei trattamenti.

6. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
7. Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare, dei ~~Referenti~~ Responsabili e dei Responsabili esterni del trattamento.

Art. 24- Responsabile della protezione dati

1. Il Titolare, con suo provvedimento, nomina il DPO (Data Protection Officer), in seguito indicato con "RPD", Responsabile comunale della protezione dei dati, sulla base delle valutazioni economico-finanziarie ed organizzative deliberate con gli strumenti di programmazione annuale.
2. La nomina presuppone l'assenza di conflitto di interessi al fine di salvaguardare gli obblighi di indipendenza del RPD.
3. Il Responsabile della protezione dei dati è individuato in un soggetto esterno al Comune, in possesso di idonee qualità professionali, con particolare

riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, all'adeguata conoscenza delle strutture organizzative degli Enti locali e delle norme e procedure amministrative agli stessi applicabili, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. I compiti attribuiti al RPD esterno sono indicati in apposito contratto di servizi o in alternativa nel decreto di nomina.

4. Il RPD esterno è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.
5. E' possibile l'affidamento dell'incarico di RPD ad un unico soggetto, anche esterno, designato da più Comuni mediante esercizio associato della funzione, nelle forme previste dal T.U. Enti Locali, approvato con D.lgs. 18.08.2000, n. 267 e s.m.i.
6. Il RPD è incaricato dei seguenti compiti:
   a) informare e fornire consulenza al Titolare ed ai Designati nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati personali. In tal senso il RPD può indicare al Titolare e/o ai Designati del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
   b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e dei Designati 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 dei Designati del trattamento;
   c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dai Designati;
   d) fornire, se richiesto, un parere scritto in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;
   e) fungere da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;

f) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD ed i dati di contatto dello stesso devono essere pubblicati sul sito istituzionale e sono comunicati a cura del Titolare del trattamento al Garante della protezione dei dati personali. Allo scopo di garantire una supervisione da parte del vertice gestionale dell'Ente, le eventuali comunicazioni formali al Garante per la protezione dei dati personali sono sottoscritte anche dal Segretario generale;
g) la tenuta, qualora richiesto, dei registri di cui agli articoli 33 e 34;
h) altri compiti e funzioni, a condizione che il Titolare o i Designati del 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 RPD.

7. Il Responsabile della protezione dei dati deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   - 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;
   - 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;
   - il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente;
   - il RPD può convocare periodicamente riunioni di coordinamento dei Referenti del trattamento designati allo scopo di trattare questioni ritenute opportune per garantire la protezione dei dati personali.
8. 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. In tal senso il RPD:
   a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
   b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed ai Referenti del trattamento interessati.
9. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
   – il Responsabile per la prevenzione della corruzione e per la trasparenza;
   – il Designati del trattamento;

- Qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

10. Da parte del Titolare e dei Designati, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente, devono essere garantite al RPD autonomia e risorse strumentali sufficienti per assolvere in modo efficace i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:
    - supporto attivo per lo svolgimento dei compiti da parte della Giunta comunale e dei referenti interni, 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;
    - supporto adeguato in termini di infrastrutture (sede, attrezzature, strumentazione);
    - 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;
    - accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali;
    - 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.
11. Il RPD non può essere rimosso o penalizzato dal Titolare a causa dell'adempimento dei propri compiti.
12. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare e al Designato del trattamento competente per materia.
13. 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 e al Designato interessato.
14. Il RPD mantiene uno stretto rapporto di collaborazione con il Segretario comunale e con il responsabile del settore preposto alla gestione dei sistemi informativi.

Art. 25 – Designati a specifici compiti e funzioni connesse al trattamento dei dati (responsabili interni)

1. Il Titolare si avvale di più Designati al trattamento dei dati che presentino garanzie sufficienti per mettere in atto misure tecniche, organizzative e di sicurezza adeguate in modo tale che il trattamento dei dati personali garantisca la tutela dei diritti dell'interessato nel rispetto del Codice, del RGPD e del presente Regolamento.

2. Allo scopo di cui al comma precedente ciascun dirigente ovvero responsabile titolare di posizione organizzativa delle strutture di massima dimensione in cui si articola l'organizzazione dell'Ente è nominato dal Sindaco, di norma, entro tre mesi dalla data della sua proclamazione, Designato a specifici compiti e funzioni connesse al trattamento dei dati. Sino a nuova designazione si intende prorogata di diritto la designazione degli stessi in carica al momento della predetta proclamazione.
3. La designazione dei Responsabili in posizioni apicali avviene con il decreto di attribuzione delle funzioni dirigenziali o con separato decreto, nel quale sono tassativamente previsti le seguenti funzioni e poteri:
   a) trattare i dati personali solo su istruzione del Titolare del trattamento e ai sensi di legge;
   b) assicurare, nell'esercizio dei compiti assegnati, il tempestivo ed integrale rispetto dei doveri del Titolare previsti dal Codice e dal RGPD;
   c) osservare le disposizioni del presente Regolamento nonché delle specifiche istruzioni impartite dal Titolare;
   d) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;
   e) collaborare con il Titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione ed aggiornamento del Registro delle attività di trattamento, in collaborazione con l'Amministratore di sistema e con le altre strutture competenti del Titolare, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;
   f) curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'organizzazione del Titolare per l'applicazione del Codice, del RGPD, e del presente Regolamento;
   g) assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;
   h) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD (notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;
   i) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel Codice, RGPD e nel presente Regolamento;

j) contribuire alle attività di verifica del rispetto del Codice, del RGPD e del presente regolamento, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato;
k) fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/PDO) nell'esercizio delle sue funzioni.

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Comune e ciascun Designato.

4. Ciascun Designato nell'espletamento dei compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, collabora con il Titolare al fine di:
   - comunicare tempestivamente l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante al riguardo;
   - proporre eventuali autorizzati a specifici trattamenti di dati personali, e fornire loro specifiche istruzioni;
   - proporre la nomina dei responsabili (esterni) del trattamento dei dati nell'ambito degli appalti di servizi;
   - garantire la sensibilizzazione e l'aggiornamento del personale che partecipa ai trattamenti ed alle connesse attività di controllo, anche richiedendo al Titolare direttamente o tramite il RPD specifica attività di formazione;
   - rispondere alle istanze degli interessati secondo quanto stabilito dal Codice e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
   - garantire che tutte le misure, tecniche ed organizzative, di sicurezza del trattamento siano applicate all'interno della propria struttura ed all'esterno, qualora vi sia trattamento di dati personali afferenti le proprie competenze da parte di soggetti terzi quali Responsabili del trattamento;
   - informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.
5. I Designati Responsabili interni del trattamento sono destinatari di interventi di formazione e di aggiornamento.

Art. 26 – Autorizzati al trattamento

1. Gli autorizzati al trattamento sono i soggetti alle dipendenze dell'Ente addetti allo svolgimento di compiti e funzioni connessi al trattamento di dati personali di competenza nell'ambito delle mansion assegnate.
2. Gli autorizzati collaborano con il Titolare ed il Designato, Responsabile in posizione apicale, segnalando eventuali situazioni di rischio nel trattamento

dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.

3. In particolare, gli autorizzati devono assicurare che, nel corso del trattamento, i dati siano:
   a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
   b) raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
   d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
   e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono trattati;
   f) trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.
4. Gli ~~autorizzati~~ sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e dal Designato nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del Titolare.
5. Gli autorizzati dipendenti del Titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 27 – Gli autorizzati al trattamento non dipendenti del Titolare

1. Tutti i soggetti che svolgono un'attività di trattamento dei dati, e che non sono dipendenti del Titolare, quali a titolo meramente esemplificativo i tirocinanti, i volontari, consulenti e i soggetti che operano temporaneamente all'interno della struttura organizzativa del Titolare così come gli incaricati nominati dai Responsabili del trattamento (esterni), devono essere autorizzati al trattamento tramite atto scritto di nomina o nell'ambito della disciplina contrattuale d'incarico.
2. Questi ultimi sono soggetti agli stessi obblighi cui sono sottoposti tutti gli autorizzati dipendenti del Titolare, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
3. Gli autorizzati non dipendenti dal Titolare possono essere comunque destinatari di interventi di formazione e di aggiornamento.

Art. 28 – Responsabili del trattamento (esterni)

1. Il Titolare su proposta dei Designati (responsabili interni) può nominare quali Responsabili esterni del trattamento di dati uno o più soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da tali soggetti esterni al Comune in virtù di convenzioni, di contratti, di appalti, di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali. In tal caso il Titolare, ai sensi dell'art. 28 del RGPD, in considerazione della complessità e della molteplicità delle funzioni istituzionali, ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative, ivi compreso il profilo relativo alla sicurezza, adeguate in modo tale che il trattamento soddisfi i requisiti dello stesso RGPD e garantisca la tutela dei diritti dell'interessato.
2. Il Responsabile esterno è il soggetto che effettua un trattamento per conto del Titolare. Ove necessario per esigenze organizzative, possono essere nominati Responsabili più soggetti, anche mediante suddivisione di compiti.
3. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare.
4. Il trattamento di dati esternamente al Titolare da parte di un Responsabile del trattamento è disciplinato da un atto che regola il rapporto tra il Titolare ed il Responsabile del trattamento e deve in particolare stabilire quanto previsto dall'art. 28, comma 3, del RGPD; tale atto può anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
5. I Responsabili esterni del trattamento hanno l'obbligo di:
   a) trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto del Codice, del RGPD e del presente Regolamento;
   b) attenersi alle disposizioni impartite dal Titolare del trattamento;
   c) rispettare le misure di sicurezza previste dal Codice sulla privacy e adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
   d) tenere per iscritto un registro di tutte le categorie di attività di trattamento effettuate per conto del Titolare e che comprendono:
      - il nome e i dati del Titolare del trattamento per conto del quale opera, degli eventuali responsabili e del responsabile della protezione dei dati;
      - le categorie di trattamenti effettuati per conto del Titolare del trattamento;
      - se applicabili, i trasferimenti di dati a carattere personale verso un paese terzo o ad una organizzazione internazionale e, nel caso di trasferimenti previsti dall'articolo 49, paragrafo 1, secondo comma

del RGPD, i documenti che attestano l'esistenza di opportune garanzie;

e) nominare al proprio interno i soggetti autorizzati del trattamento;
f) garantire che i dati trattati siano portati a conoscenza soltanto del personale autorizzato del trattamento;
g) assistere il Titolare nella realizzazione di analisi di impatto relative alla protezione dei dati, conformemente all'articolo 35 del RGPD. Il Responsabile del trattamento assiste il Titolare nella consultazione preventiva dell'autorità di controllo, prevista dall'articolo 36 dello stesso RGPD;
h) adottare le misure adeguate di sicurezza necessarie per garantire la riservatezza e la protezione dei dati personali trattati;
i) specificare, se richiesti dal Titolare, le misure adottate di cui al punto precedente ed i luoghi dove fisicamente avviene il trattamento dei dati;
j) il Responsabile del trattamento notifica al Titolare ogni violazione di dati a carattere personale nel tempo massimo di 24 ore dopo esserne venuto a conoscenza, per via telefonica e pec. Tale notifica è accompagnata da ogni documentazione utile per permettere al Titolare, se necessario, di notificare questa violazione all'Autorità di controllo competente.

6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
7. Nel caso di mancato rispetto delle predette disposizioni, e in caso di mancata comunicazione al Titolare dell'atto di nomina di eventuali soggetti designati al trattamento dei dati, ne risponde direttamente, verso il Titolare, il Responsabile esterno del trattamento.

Art. 29 – Amministratore di sistema

1. L'Amministratore di sistema, ovvero il soggetto cui sono affidati i privilegi di Amministratore del sistema informatico (persona fisica), è la figura professionale che sovraintende alla gestione ed alla manutenzione di sistemi di elaborazione di cui è dotata l'Amministrazione, con particolare riferimento alla configurazione degli stessi, nonché alla gestione e alla manutenzione delle banche dati. Nell'ambito dell'organizzazione è possibile individuare tipologie specifiche di amministratore di sistema, differenziate per livello di autorizzazione e profilo.
2. L'attribuzione delle funzioni di gestore dei privilegi di amministratore del sistema informatico avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto della normativa in vigore sul trattamento dei dati e sulla sicurezza informatica. La designazione dell'Amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

3. L'Amministratore di sistema svolge attività, quali, a titolo esemplificativo e non esaustivo:
    a) pianificare, eseguire e verificare l'organizzazione dei flussi di rete, la corretta esecuzione del backup e delle copie, la gestione dei supporti di memorizzazione e la manutenzione hardware;
    b) proporre l'introduzione ed integrazione di nuove tecnologie negli ambienti esistenti;
    c) installare e configurare nuovo hardware/software sia lato client che lato server;
    d) applicare le patch e gli aggiornamenti necessari al software di base applicativo, modificare la configurazione in base all'esigenze della Amministrazione;
    e) gestire e mantenere aggiornati gli account utente relativi ai profili di autorizzazione;
    f) fornire risposte a questioni tecniche di competenza sollevate dagli utenti;
    g) affrontare ed attivarsi per risolvere problemi, guasti o malfunzionamenti.
4. Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'Amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.
5. Secondo la normativa vigente, l'operato dell'Amministratore di sistema deve essere verificato, con cadenza annuale, da parte del Titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.
6. Il Titolare di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
7. L'Amministratore di sistema è destinatario degli interventi di formazione e di aggiornamento.

Art. 30 - Coordinamento con Amministrazione trasparente, procedimenti di accesso civico, generalizzato e documentale

1. Costituisce onere sia del RPD che del Responsabile comunale per la prevenzione della corruzione e della trasparenza coordinare le loro attività al fine di semplificare e minimizzare l'impatto degli adempimenti sull'attività degli uffici/servizi e garantire la massima protezione dei dati personali ogni qualvolta procedimenti di ufficio o attivati su istanza di soggetti esterni

comportino attività di pubblicazione dei dati personali in Amministrazione trasparente, il rilascio di dati personali in occasione di istanze di accesso civico, generalizzato e documentale. In tali ultime ipotesi dovranno essere adottate misure di sicurezza adeguate compresa la minimizzazione dei dati personali.

2. Negli atti destinati alla pubblicazione o divulgazione, i dati che permettono di identificare gli interessati sono riportati quando è necessario ed è previsto da una norma di legge mentre in tutti gli altri casi ciò deve avvenire rispettando il principio di proporzionalità, mediante la verifica che tale pubblicazione a fini di trasparenza concerne solo dati pertinenti e non eccedenti rispetto alle finalità perseguite.

Art. 31 - Attività amministrativa

1. L'attività amministrativa del Comune si svolge, principalmente, con la emissione, la elaborazione, la riproduzione e la trasmissione di dati, compresi i procedimenti per la emanazione di provvedimenti, mediante sistemi informatici o telematici.
2. Tutta l'attività di gestione dei dati deve essere pertanto ispirata a:
    a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati;
    b) prevenire:
        - trattamenti dei dati non conformi alla legge o ai regolamenti;
        - cessione o distribuzione dei dati in caso di cessazione del trattamento.
3. Per l'attività informatica di cui al comma 1 sono rispettate le norme di cui al codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni ed integrazioni.
4. La sicurezza dei dati personali è assicurata anche mediante adeguate soluzioni tecniche connesse all'utilizzo della firma digitale, chiavi biometriche o altre soluzioni tecniche.

Art. 32 - Sicurezza del trattamento

1. Il livello di sicurezza da assicurare nel trattamento dei dati è valutato tenuto conto dei rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
2. Il Comune di _____, ciascun Designato e ciascun Responsabile del trattamento, anche in relazione alle conoscenze acquisite in base al progresso tecnologico, 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.

3. Le misure tecniche ed organizzative di sicurezza utilizzabili da parte dei soggetti di cui al comma precedente 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.
4. Costituiscono inoltre misure tecniche ed organizzative che possono essere adottate dal servizio cui è preposto ciascun Designato (responsabile interno) del trattamento:
   - sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
   - sistemi di rilevazione di intrusione; sistemi di sorveglianza; 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.
5. Il Titolare e ciascun Responsabile del trattamento sono tenuti ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
6. Restano in vigore le misure di sicurezza attualmente previste, le limitazioni alla diffuzione e alla pubblicazione per i trattamenti di particolari tiologie di dati, c.d. dati sensibili, per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi.

Art. 33 - Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
   a) il nome ed i dati di contatto del Comune, del Titolare, eventualmente del ConTitolare del trattamento, 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;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente articolo 32.

2. Il Registro unico del trattamento è tenuto dal Titolare, presso la sede del Comune in forma telematica/cartacea; nello stesso possono essere inserite ulteriori informazioni tenuto conto di specifiche necessità organizzative e funzionali dell'Ente.
3. Nel caso di cui al precedente comma, il Titolare può, sotto la propria responsabilità, decidere di affidare la tenuta di tale registro unico al RPD. Ciascun Designato ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico. Resta, invece, fermo l'obbligo per i Responsabili esterni del trattamento di tenere distintamente il registro delle attività di trattamento ed il registro delle categorie di attività trattate.

Art. 34 - Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Designato del trattamento reca le seguenti informazioni:
   i. il nome ed i dati di contatto del Designato del RPD;
   ii. le categorie di trattamenti effettuati da ciascun Designato o 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;
   iii. l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   iv. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente articolo 32.

Art. 35 - Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, in particolare allorché questo 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 del 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, del 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, del

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 del 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 esso 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.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune.
Il Titolare può 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.

5. Il Designato del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.
6. L'ufficio comunale competente per la sicurezza dei sistemi informativi fornisce supporto al Titolare per lo svolgimento della DPIA.
7. 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.
8. La DPIA non è necessaria nei casi seguenti:
    i. 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, del RGDP;
    ii. 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;
    iii. 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;
    iv. 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.
9. 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. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.
10. 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.

11. 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.
12. 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.
13. 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. 36- 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 dal Titolare.
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 dal primo accertamento del verificarsi dell'evento e comunque senza ingiustificato ritardo.

3. Il Responsabile esterno del trattamento notifica al Titolare ogni violazione di dati a carattere personale nel tempo massimo di 24 ore, a mezzo pec. I Designati sono obbligati ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuti a conoscenza della violazione.
4. 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:
    A. danni fisici, materiali o immateriali alle persone fisiche;
    B. perdita del controllo dei dati personali;
    C. limitazione dei diritti, discriminazione;
    D. furto o usurpazione d'identità;
    E. perdite finanziarie, danno economico o sociale.
    F. decifratura non autorizzata della pseudonimizzazione;
    G. pregiudizio alla reputazione;
    H. perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
5. 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:
    a. coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
    b. riguardare categorie particolari di dati personali
    c. comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze)
    d. 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);
    e. impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).
6. 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.
7. Il Titolare deve opportunamente documentare, mediante la istituzione di un registro, 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. 37 – Pubblicazione sintesi della valutazione d'impatto – DPIA

1. Il Titolare effettua la pubblicazione della DPIA o di una sintesi della stessa al fine di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal Titolare, nonché di dimostrare la responsabilizzazione e la trasparenza.
2. La DPIA pubblicata non deve contenere l'intera valutazione qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il Titolare o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della DPIA o addirittura soltanto in una dichiarazione nella quale si afferma che la DPIA è stata condotta.

Art. 38 – Consultazione preventiva

1. Il Titolare, prima di procedere al trattamento dei dati, consulta, per il tramite del RPD/PDO, il Garante qualora la valutazione d'impatto sulla protezione dei dati abbia evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adottate.

Art. 39 – Modulistica e procedure

1. Il Titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del Codice, del RGPD, del presente Regolamento, e di tutte le linee guida e provvedimenti del Garante
   a) adotta e costantemente aggiorna:
      - modelli uniformi di informativa;
      - modelli e formule uniformi necessarie per gestire il trattamento dei dati e le misure di sicurezza;
   b) elabora, approva, e costantemente aggiorna adeguate procedure gestionali.

Art. 40 – Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

1. Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è sanzionato con le sanzioni previste da parte del Garante, nonché con sanzioni di natura disciplinare.
2. Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento.
3. Il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi previsti nel Codice, nel RGPD e nel presente regolamento, e a lui specificamente diretti o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal Titolare del trattamento.
4. Il Titolare e il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo loro imputabile.

Art. 41 – Principio di collaborazione

1. Tutto il personale coinvolto nelle procedure di trattamento dati, a qualunque livello e ruolo:
   i. collabora con il Titolare, il RPD, l'Autorità di controllo ed eventuali ulteriori soggetti addetti alla vigilanza, controllo ed attuazione delle disposizioni in materia di trattamento dei dati fornendo la massima e tempestiva collaborazione con particolare riferimento al rispetto dei principi previsti dal RGPD;
   ii. fornisce tempestivamente informazioni su potenziali pericoli, rischi, o violazioni dei dati personali anche al fine di consentire l'esercizio dei compiti di cui all'art. 33 e 34 del RGPD (cosiddetto "data breach");
   iii. collabora con i Designati del trattamento, secondo le istruzioni fornite dal Titolare, al fine di garantire le citate finalità e nel rispetto degli obblighi di segretezza e riservatezza.
   iv. si impegna a rispettare le previsioni normative di livello europeo, nazionale e regolamentare per la tutela dei dati personali.
2. Il rispetto dei principi in materia e dei compiti e adempimenti previsti dal presente provvedimento verrà valutato in sede di raggiungimento degli obiettivi e/o negli altri casi di responsabilità del personale a vario titolo coinvolto.

Art. 42 – Disposizioni finali

1. Per quanto non previsto nel presente Regolamento, si rinvia al “Regolamento generale sulla protezione dei dati (UE)2016/679”, alle vigenti fonti di diritto europee e nazionali, con particolare riferimento al dlgs 196/2003 e ai regolamenti comunali in materia di protezione dei dati personali, alle linee guida e ai provvedimenti del “Gruppo di Lavoro 29” nonché del Garante della Privacy, alle direttive impartite dal Titolare del trattamento e dai Responsabili del trattamento, dall’Amministratore del sistema informatico e dal Responsabile della protezione dei dati.

COMUNE DI _____

PROVINCIA DI

BOZZA REGOLAMENTO PER LA DISCIPLINA ED UTILIZZO DEGLI IMPIANTI DI VIDEOSORVEGLIANZA E FOTOTRAPPOLAGGIO

Approvato con deliberazione di Consiglio Comunale n._ del_____

INDICE

PREMESSA

Il presente Regolamento è redatto a norma del:

1. Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), e del Decreto Legislativo 10 agosto 2018, n° 101, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, che modifica e integra il dlgs 196/2003 Codice nazionale sulla privacy";
2. Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15, "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia", nonché il DL n. 51/2018 che recepisce la Direttiva Europea 680/2016, "Relativa alla protezione delle persone fisiche 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".

CAPO I DISPOSIZIONI GENERALI

Art. 1 - Oggetto

1. Il presente Regolamento disciplina il trattamento, interamente o parzialmente automatizzato, dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e fototrappolaggio attivati nel territorio dell'Ente determinandone le condizioni necessarie per la tenuta in esercizio, ai sensi del Reg. UE 2016/679, della Direttiva UE 2016/680, in osservanza delle disposizioni contenuti nel "decalogo" del 8 aprile 2010 dal Garante della Privacy.

2. L'installazione e l'attivazione degli impianti non deve essere sottoposto all'esame preventivo del Garante ma è sufficiente che il trattamento dei dati personali effettuato per lo svolgimento dei propri compiti istituzionali avvenga previa informativa alle persone che stanno per accedere nell'aree sorvegliate, con apposita segnaletica come individuata dal Garante, e siano adottate idonee misure di sicurezza.

3. In particolare il presente Regolamento:

a. Disciplina utilizzo degli impianti di videosorveglianza fissi, mobili, di lettura targhe e fototrappole di proprietà dell'Ente o da esso gestiti;

b. Definisce le caratteristiche e le modalità di utilizzo degli impianti;

c. Disciplina gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti.

4. Gli impianti:

a. Riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese;

b. Consentono riprese unicamente di video o foto;

c. Sono installati nel territorio dell'Ente;

d. Sono gestiti dal Responsabile della gestione tecnica degli impianti designato a norma dell'articolo 6 del presente regolamento.

5. Sono attivabili impianti videosorveglianza e fototrappolaggio fissi e mobili, posizionabili in aree del territorio dell'Ente oppure montate su veicoli di servizio.

6. Il sistema di videosorveglianza dell'Ente è integrato con le apparecchiature di rilevazione della targa dei veicoli in transito, apposte lungo i varchi di accesso perimetrali alla rete viaria cittadina, ai fini della sicurezza urbana. La disciplina relativa al trattamento dati di cui al presente Regolamento si applica a tali apparecchi, in quanto e nei limiti in cui consentono la ripresa delle immagini e la registrazione dei dati alfanumerici contenuti nelle targhe veicolari.

7. L'utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della Strada, in considerazione della peculiarità dei fini istituzionali perseguiti, non è assoggettato alla disciplina di cui al presente Regolamento, ma alle disposizioni dettate dal Garante della privacy nel decalogo del 8 aprile 2010 al paragrafo 5.3 nonché dalla specifica normativa di settore vigente.

Art. 2 - Definizioni

1. Ai fini del presente Regolamento si intende:

   a. Per “Codice”, il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196 novellato dal D.Lgs 118/2011 e successive modificazioni ed integrazioni;

   b. Per “impianto di videosorveglianza e fototrappolaggio”, qualunque impianto di ripresa, fissa o mobile, composto da una o più telecamere, in grado di riprendere, registrare immagini, suoni e scattare fotografie, utilizzato per le finalità indicate dall’articolo 3 del presente Regolamento;

   c. Per “banca dati”, il complesso di dati personali acquisiti mediante l’utilizzo degli impianti di videosorveglianza;

   d. Per “trattamento”, qualunque operazione o complesso di operazioni, svolti anche con l’ausilio dei mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l’organizzazione, la conservazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, l’interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione di dati personali;

   e. Per “dato personale”, qualunque informazione relativa a persona fisica, identificata o identificabile anche indirettamente e rilevata con trattamenti di immagini effettuati mediante gli impianti;

   f. Per “Titolare del trattamento dei dati personali”, il Legale Rappresentante dell’Ente protempore, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;

   g. Per “Responsabile del trattamento dei dati personali”, la persona fisica, legata da rapporto di servizio al titolare e preposta dal medesimo al trattamento dei dati personali formalmente nominata;

   h. Per “Responsabile della gestione tecnica degli impianti di videosorveglianza”, la persona fisica o giuridica, legata da rapporto di servizio al titolare e preposta dal medesimo, o dal Responsabile dei trattamento del Servizio di riferimenti, all’installazione, all’utilizzo ed alla manutenzione degli impianti di videosorveglianza formalmente nominata;

   i. Per “Autorizzati al trattamento”, le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile del trattamento dei dati personali formalmente nominate;

   j. Per “interessato”, la persona fisica a cui si riferiscono i dati personali;

   k. Per “comunicazione”, il dare conoscenza dei dati personali ad uno o più soggetti determinati diversi dall’interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

   l. Per “diffusione”, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m. Per “dato anonimo”, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

n. Per “blocco”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

Art. 3 - Finalità

1. Le finalità di utilizzo degli impianti di videosorveglianza e fototrappolaggio di cui al presente regolamento sono conformi alle funzioni istituzionali demandate all’Ente, dalla normativa vigente, dallo Statuto e dai Regolamenti, nonché dal Decreto Legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 “Disposizioni urgenti in materia di sicurezza delle città” e dalle altre disposizioni normative applicabili all’Ente in tema di sicurezza e presidio del territorio. In particolare, l’uso di questi impianti è strumento per l’attuazione di un sistema integrato di politiche per la sicurezza urbana, di cui alle fonti normative sopra citate.

2. L’utilizzo degli impianti è finalizzato a:

a. Attività di prevenzione, indagine, accertamento e perseguimento di atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell’ambito del più ampio concetto di “sicurezza urbana” di cui all’articolo 4 del decreto legge n. 14/2017 e s.m.i., delle attribuzioni del Sindaco in qualità di autorità locale di cui all’art. 50 e di ufficiale di governo di cui all’art. 54 comma 4 e 4-bis del dlgs 267/2000;

b. Prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado, di discarica di materiale e di sostanze pericolose o di abbandono di rifiuti, e svolgere i controlli volti ad accertare e sanzionare le violazioni delle norme contenute nel regolamento di polizia urbana, nei Regolamenti locali in genere e nelle Ordinanze Sindacali;

c. Vigilare sull’integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;

d. Tutelare l’ordine, il decoro e la quiete pubblica;

e. Controllare aree specifiche del territorio comunale;

f. Monitorare e controllare la viabilità e i flussi di traffico;

g. Verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici;

h. Coordinamento delle attività di protezione civile.

3. Ai sensi di quanto previsto dall’articolo 4 della Legge 20 maggio 1970 n. 300 e s.m.i., gli impianti di videosorveglianza non possono essere utilizzati per effettuare controlli sull’attività lavorativa dei dipendenti dell’Ente, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

Art. 4 - Principi applicabili al trattamento dei dati personali

1. Il presente Regolamento garantisce che il trattamento dei dati personali, acquisiti mediante l’utilizzo degli impianti di videosorveglianza e di fototrappolaggio gestiti dall’Ente e collegati alle centrali di controllo ubicate presso gli Uffici dell'Ente, si svolga nel rispetto dei diritti, delle libertà

fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce al contempo il rispetto dei diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento.

2. L'utilizzo degli impianti comporta esclusivamente il trattamento di dati personali rilevati mediante le riprese video e foto che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area oggetto di sorveglianza.

3. Il trattamento dei dati personali si svolge nel pieno rispetto dei principi di liceità, finalità, limitazione pertinenza e proporzionalità, sanciti dal Codice Privacy novellato e dal Reg. UE2016/679.

4. In attuazione dei principi di liceità e finalità, il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza è effettuato dall'Ente esclusivamente per lo svolgimento delle funzioni istituzionali e per il perseguimento delle finalità di cui all'articolo 3 del presente Regolamento.

5. In attuazione del principio di limitazione e pertinenza, gli impianti di videosorveglianza, fototrappolaggio e i programmi informatici di gestione sono configurati in modo da ridurre al minimo l'uso di dati personali ed identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi o con modalità che permettano di identificare l'interessato solo in caso di necessità, sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti.

CAPO II SOGGETTI

Art. 5 - Titolare

1. L'Ente, nella persona del Sindaco pro tempore, è Titolare del trattamento dei dati personali acquisiti mediante utilizzo degli impianti di videosorveglianza e fototrappolaggio di cui al presente Regolamento, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza.

2. Il Titolare del trattamento dei dati personali acquisiti anche mediante l'utilizzo di questi impianti:

a. Definisce le linee organizzative per l'applicazione della normativa di settore;

b. Effettua le notificazioni al Garante per la protezione dei dati personali;

c. Nomina i Designati al trattamento dei dati impartendo istruzioni ed assegnando compiti e responsabilità;

d. Nomina i Responsabili del trattamento dei dati personali impartendo istruzioni ed assegnando compiti e responsabilità;

e. Detta le "Linee Guida" di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza;

f. Vigila sulla puntuale osservanza delle disposizioni impartite;

g. Nello svolgimento delle attività pertinenti si avvale del supporto del Responsabile della protezione dei dati personali.

Art. 6 – Designati a specifici trattamenti dei dati (responsabili interni)

1. La Responsabilità della gestione tecnica e manutenzione degli impianti di videosorveglianza e fototrappolaggio sono affidati con decreto Sindacale al Responsabile della Servizio di Polizia Locale o facente funzioni tramite apposita designazione.

2. Il Responsabile (designato) effettua il trattamento nel rispetto della normativa vigente in materia di protezione dei dati personali, ivi incluso il profilo della sicurezza e delle disposizioni del presente Regolamento.

3. Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal Titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle proprie disposizioni ed istruzioni.

4. Il Responsabile e il personale interno, se specificatamente autorizzato (incaricato), in relazione all'utilizzo degli impianti:

a. Adottano le misure e dispongono gli interventi necessari per la sicurezza del trattamento dei dati e la correttezza dell'accesso ai dati;

b. Curano la gestione delle modalità di ripresa e di registrazione delle immagini;

c. Collaborano con il Responsabile per la protezione dei dati per l'evasione delle richieste di esercizio dei diritti degli interessati;

d. Custodiscono le chiavi di accesso ai locali delle centrali di controllo e le chiavi dei locali e degli armadi nei quali sono custoditi i supporti contenenti le registrazioni.

Art. 7 - Responsabili esterni del trattamento dei dati

1. Il Titolare su proposta del Designato al trattamento (responsabile interno) può individuare soggetti esterni all'Ente quali Responsabili esterni del trattamento dei dati personali, nell'ambito degli appalti di forniture e servizi relativi alla installazione e manutenzione degli impianti. La nomina è effettuata con una specifica comunicazione o può essere riportata nel contratto di appalto, nel quale sono analiticamente specificati i compiti affidati ai Responsabili esterni.

3. Il Responsabile esterno degli impianti:

a. Cura l'installazione e gestisce la manutenzione degli impianti di videosorveglianza;

b. Assegna e custodisce le credenziali di accesso necessarie per l'utilizzo degli impianti di videosorveglianza.

Art. 8 - Personale autorizzato al trattamento dei dati personali

1. Il Titolare su proposta del Designato al trattamento (responsabile interno) può nominare il personale specificatamente autorizzato (incaricato) in numero sufficiente a garantire il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e fototrappolaggio di cui al presente Regolamento. La nomina è effettuata con atto scritto, nel quale sono analiticamente specificati i compiti affidati agli incaricati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati.

2. Gli autorizzati sono nominati tra i dipendenti dell'Ente che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

3. Gli autorizzati effettuano il trattamento attenendosi scrupolosamente alle istruzioni impartite dal Titolare e dai Responsabili.

4. Nell'ambito degli autorizzati sono nominati i soggetti ai quali sono affidate la custodia e la conservazione delle chiavi di accesso ai locali delle centrali di controllo e delle chiavi dei locali e degli armadi nei quali sono custoditi i supporti contenenti le registrazioni.

Art. 9 - Soggetti esterni

1. Ai soggetti esterni all'Ente e dei quali questo si avvale a qualsiasi titolo per lo svolgimento di servizi e attività per le quali si trattano dati personali acquisiti mediante l'utilizzo degli impianti di cui al presente regolamento, si applica la disposizione dell'articolo 5 del Regolamento per la tutela della riservatezza dei dati personali.

CAPO III TRATTAMENTO DEI DATI PERSONALI

Art. 10 - Modalità di raccolta e requisiti dei dati personali

1. I dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e fototrappolaggio di cui al presente regolamento sono:

a. Trattati in modo lecito e secondo correttezza;

b. Raccolti e registrati per le finalità di cui all'articolo 3 del presente Regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;

c. Esatti e, se necessario, aggiornati;

d. Trattati in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti.

2. Gli impianti di cui al presente Regolamento consentono riprese video e foto a colori, diurne e notturne, in condizioni di sufficiente illuminazione naturale o artificiale. Non sono effettuate riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali al soddisfacimento delle finalità di cui all'articolo 3 del presente Regolamento.

3. Gli impianti di videosorveglianza sono sempre in funzione e registrano in maniera continuativa, mentre gli impianti di fototrappolaggio si innescano in modo autonomo a seguito di qualsiasi movimento di veicoli o esseri umani catturando immagini.

4. I segnali video e foto delle unità di ripresa sono inviati presso la sede comunale o data center individuato appositamente dove sono registrati su appositi server. In queste sedi le immagini sono visualizzate su monitor e hardware client appositamente configurato il cui accesso è protetto, riservato e consentito unicamente al personale formalmente e appositamente incaricato. L'impiego del sistema di videoregistrazione e foto è necessario per ricostruire l'evento, ai fini del soddisfacimento delle finalità di cui all'articolo 3 del presente Regolamento.

Art. 11 - Conservazione dei dati personali

1. I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione. Decorso tale periodo, i dati registrati sono cancellati con modalità automatica. Gli strumenti e i supporti elettronici utilizzati sono dotati dei sistemi di protezioni che garantiscono la tutela dei dati trattati.

2. La conservazione dei dati personali per un periodo di tempo superiore a quello indicato dal comma 1 del presente articolo è ammessa esclusivamente su specifica richiesta della Autorità Giudiziaria o di Polizia Giudiziaria in relazione ad un'attività investigativa in corso.

3. In tali casi dovrà essere informato il Responsabile del trattamento degli impianti di cui al presente Regolamento, che darà esplicita autorizzazione al soggetto di cui all'art. 6 ad operare per tale fine.

4. Fuori delle ipotesi espressamente previste dal comma 2 del presente articolo, la conservazione dei dati personali per un tempo eccedente i sette giorni è subordinata ad una verifica preliminare del Garante per la protezione dei dati personali.

Art. 12 - Obblighi connessi al trattamento dei dati personali

1. L'utilizzo delle immagini degli impianti di videosorveglianza e fototrappolaggio da parte degli incaricati avviene nel rispetto dei limiti previsti dal presente Regolamento.

2. L'utilizzo degli impianti è consentito esclusivamente per il controllo di quanto si svolge nei luoghi pubblici mentre esso non è ammesso nelle proprietà private, se non ad uso pubblico e comunque previa sottoscrizione di convenzione tra le parti.

3. Fatti salvi i casi di richiesta degli interessati, i dati personali registrati mediante l'utilizzo degli impianti possono essere riesaminati, nel limite di tempo di sette giorni previsto per la conservazione, esclusivamente dal personale addetto in caso di effettiva necessità e per il soddisfacimento delle finalità di cui all'articolo 3 del presente Regolamento solo a fini di indagine giudiziaria o di polizia.

4. La mancata osservanza degli obblighi previsti dal presente articolo può comportare l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative, oltre che l'avvio di eventuali procedimenti penali.

Art. 13 - Informativa

1. Fermo quanto previsto dal comma 1 del presente articolo, l'Ente rende noto agli interessati il funzionamento degli impianti di videosorveglianza tramite le seguenti forme semplificate di informativa:

a. Pubblicazione sul sito internet istituzionale di planimetrie e di altra documentazione relative alle zone videosorvegliate;

b. Cartelli di cui all'informazione minima prevista dall'art. 13 comma del Reg. UE 2016/679 installati nelle aree in prossimità degli impianti.

3. L'informativa di cui sopra non è dovuta nel caso di utilizzo di telecamere a scopo investigativo a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati.

4. Fermo quanto previsto dal comma 1 del presente articolo, l'Ente rende noto agli interessati il funzionamento degli impianti di videosorveglianza installati all'interno di edifici comunali e nei pressi dei dispositivi di rilevazione tramite posizionamento di cartelli contenenti l'informativa di cui all'art. 13 del Reg. UE 2016/679.

Art. 14 - Comunicazione e diffusione dei dati personali

1. La comunicazione dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e fototrappolaggio di cui al presente Regolamento, da parte dell'Ente a favore di altri soggetti o autorità pubbliche è ammessa quando è prevista da una specifica norma di legge o regolamento anche mediante la stipula di precisi protocolli d'intesa. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali.

2. Ai sensi e per gli effetti del comma 1 del presente articolo, non si considera comunicazione la conoscenza dei dati personali da parte dei soggetti formalmente incaricati e autorizzati a compiere operazioni di trattamento dal Titolare o dai Responsabili e che operano sotto la loro diretta autorità.

3. È in ogni caso è fatta salva la comunicazione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Art. 15 - Utilizzo di particolari sistemi mobili

1. Per specifiche finalità gli operatori autorizzati o il Responsabile del trattamento di cui al presente Regolamento possono essere dotati di sistemi di microtelecamere per l'eventuale ripresa di situazioni di criticità per la sicurezza. L'utilizzo di tali sistemi, da parte degli operatori, dovrà essere disciplinato con specifiche disposizioni operative. Tali sistemi devono essere finalizzati alla tutela dell'ordine e della sicurezza pubblica, alla prevenzione, all'accertamento e alla repressione dei reati.

2. Le videocamere e le schede di memoria di cui sono dotati i sistemi di cui al comma precedente dovranno essere contraddistinte da un numero seriale che dovrà essere annotato in apposito registro recante il giorno, l'orario, i dati indicativi del servizio e la qualifica e nominativo del

dipendente che firmerà la presa in carico e la restituzione. La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato. Il sistema di registrazione dovrà essere attivato solo in caso dì effettiva necessità, ossia nel caso di insorgenza delle situazioni descritte al comma 1.

3. Spetta all'ufficiale di Polizia Giudiziaria che impiega direttamente il reparto operativo impartire l'ordine di attivazione dei dispositivi, in relazione all'evolversi degli scenari di sicurezza e ordine pubblico che facciano presupporre criticità. Lo stesso ne disporrà la disattivazione. Al termine del servizio gli operatori interessati, previa compilazione di un foglio di consegna, affideranno tutta la documentazione video realizzata al Responsabile.

4. Il trattamento dei dati personali effettuati con simili sistemi di ripresa devono rispettare i principi di cui alla Direttiva UE 2016/680 ed in particolare i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, per poi essere cancellati.

Art. 16 - Cessazione del trattamento dei dati personali

1. In caso di cessazione, per qualsiasi causa, del trattamento, i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono distrutti.

Art. 17 - Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:

a. Di ottenere la conferma dell'esistenza di trattamenti di dati che possono riguardarlo;

b. Di essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;

c. Di richiedere su richiesta avanzata prima dello spirare del termine massimo di conservazione del dato e di ottenere, senza ritardo e comunque non oltre 30 giorni dal responsabile designato:

   - La conferma dell'esistenza o meno di dati personali che lo riguardano, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento;

   - La cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati, valutate le preminenti esigenze di polizia giudiziaria e di indagine.

d. Di opporsi, in tutto o in parte, per motivi legittimi qualora sia possibile, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

2. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

3. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.

4. Le istanze di cui al presente articolo possono essere trasmesse al titolare o al responsabile anche mediante lettera raccomandata o posta elettronica certificata.

5. Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

6. Possono essere adottate misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di:

a. Non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
b. Non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;
c. Proteggere la sicurezza pubblica;
d. Proteggere la sicurezza nazionale;
e. Proteggere i diritti e le libertà altrui.

CAPO IV MISURE DI SICUREZZA

Art. 18 - Sicurezza dei dati personali

1. Ai sensi di quanto previsto dall'articolo 24 del Reg. UE 2016/679, i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e fototrappolaggio di cui al presente Regolamento sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di cui all'articolo 3 del presente Regolamento.
2. Ai sensi dell'art. 29 c. 2 della Direttiva UE 2016/680 il Titolare del trattamento, previa valutazione dei rischi, mette in atto 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 verificare e accertare gli organismi 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»);
j. 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»).

Art. 19 - Accesso alle centrali di controllo

1. I dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e fototrappolaggio di cui al presente regolamento sono custoditi, ai sensi e per gli effetti dell'articolo 11, presso il data center e le centrali di controllo ubicate presso l'Ente, nonché presso eventuali altre sedi collegate;

2. L'accesso alle centrali di controllo è consentito esclusivamente al Titolare, ai Responsabili e agli incaricati.

3. L'accesso da parte di soggetti diversi da quelli indicati al comma 2 del presente articolo è subordinato al rilascio, da parte del Titolare o dei Responsabili, di un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso.

4. Un file di log, generato automaticamente dal sistema informatico, consente di registrare gli accessi logici effettuati dai singoli operatori, le operazioni dagli stessi compiute sulle immagini registrate ed i relativi riferimenti temporali. Tale file non è soggetto a cancellazione.

5. I responsabili impartiscono idonee istruzioni atte ad evitare assunzioni o rilevamenti di dati da parte dei soggetti autorizzati all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.

6. Gli Autorizzati designati vigilano sul puntuale rispetto delle istruzioni impartite dai responsabili e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Art. 20 - Accesso agli impianti e credenziali

1. L'accesso agli impianti di videosorveglianza e fototrappolaggio può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate dal Responsabile della gestione tecnica degli impianti.

CAPO V SISTEMI INTEGRATI DI VIDEOSORVEGLIANZA

Art. 21 - Sistema integrato di videosorveglianza tra pubblico e privato

1. Al fine di promuovere la sicurezza integrata sul territorio, recependo i contenuti del decreto legge 14/2017 convertito in legge 48/2017 "disposizioni urgenti in materia di sicurezza delle città" e s.m.i., in particolare rispetto le previsioni di cui all'art. 7 dello stesso, possono essere individuati specifici obiettivi per incrementare il controllo del territorio attraverso il concorso, sotto il profilo di sostegno strumentale, finanziario e logistico, di soggetti pubblici e privati. Tali obiettivi sono individuati nell'ambito dei "patti per l'attuazione della sicurezza urbana" di cui all'art. 5 del predetto decreto, nel rispetto delle linee guida adottate.

2. Oltre all'ipotesi di cui al comma precedente, potranno essere attivate le seguenti tipologie di sistemi integrati, previa sottoscrizione di un protocollo di gestione:

a. Gestione coordinata di funzioni e servizi tramite condivisione delle immagini riprese da parte di diversi e autonomi Titolari del trattamento, utilizzanti le medesime infrastrutture tecnologiche;

b. Collegamento telematico di diversi Titolari di trattamento ad un "centro" unico gestito da soggetto terzo;

c. Collegamento del sistema di videosorveglianza con la sala operativa degli Organi di Polizia di Stato.

3. L'utilizzo di sistemi integrati di videosorveglianza, ivi compresi quelli che consentono di rendere disponibili le immagini alle Forze di Polizia di Stato devono avere le specifiche misure che prevedono:

a. L'adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei Responsabili da parte del Titolare;

b. La separazione logica delle immagini registrate dai diversi titolari.

4. In qualunque caso le modalità di trattamento dei dati dovranno essere conformi alle prescrizioni date dal Garante della protezione dei dati personali. Con specifico riferimento all'attività del controllo sul territorio da parte dei Comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale per finalità di sicurezza urbana:

a. L'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica sia configurato con modalità tali da permettere ad ogni singolo Ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'Ente;

b. Un centro unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, in tale caso i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola Pubblica Amministrazione.

CAPO VI TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art. 22 - Tutela

1 In sede amministrativa, il Responsabile del procedimento amministrativo, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il Designato al trattamento dei dati personali, così come individuato dal precedente articolo 7.

CAPO VII DISPOSIZIONI FINALI

Art. 23 - Aggiornamento elenco impianti

1. L'aggiornamento dell'elenco degli impianti di videosorveglianza e fototrappolaggio è demandato al Responsabile della gestione tecnica degli impianti di cui al presente Regolamento, sulla base di provvedimenti che ne avallano la scelta.

2. Ai fini dell'attuazione del comma 1 del presente articolo, il Responsabile della gestione tecnica degli impianti segnala tempestivamente al Titolare del trattamento dati l'installazione e l'attivazione di nuovi impianti e le modifiche alle caratteristiche o alle modalità di utilizzo degli impianti già installati.

Art. 24 - Obblighi di preventivo esame

1. L'installazione e l'attivazione del sistema di videosorveglianza e il presente Regolamento non devono essere sottoposti all'esame preventivo del Garante, essendo sufficiente che il trattamento dei dati personali effettuato tramite tale sistema sia finalizzato per lo svolgimento dei propri compiti istituzionali ed avvenga previa informativa alle persone che stanno per accedere nell'area videosorvegliata e siano adottate idonee misure di sicurezza.

Art. 25 - Norma di rinvio

1. Per quanto non espressamente disciplinato dal presente Regolamento, si rinvia al Reg. UE 2016/679 e al Codice Privacy novellato, al dlgs 196/2003 aggiornato, al provvedimento in materia di videosorveglianza emanato dal Garante per la protezione dei dati personali in data 8 aprile 2010, nonché alle altre disposizioni normative vigenti in materia.

2. Il presente Regolamento esplica i propri effetti al momento dell'eseguibilità della delibera di approvazione da parte dell'Organo Consigliare.

OGGETTO: CONVENZIONE TRA IL COMUNE DI _____ E LA STAZIONE DEI CARABINIERI DI _____ PER LA CONDIVISIONE DELLE IMMAGINI DELLE TELECAMERE DELLA VIDEOSORVEGLIANZA INSTALLATE NEL TERRITORIO DEL COMUNE

Premesso che:

- Il Regolamento Comunale per la Videosorveglianza e il Fototrappolaggio approvato con Delibera del Consiglio Comunale n. __ del _____ prevede la possibilità di collegare le telecamere della videosorveglianza con le altre Forze di Polizia;
- Il Comune di _____, nella persona del Sindaco pro tempore, e la Stazione Carabinieri di _____, nella personale del Comandante pro tempore, intendono concordare mirate iniziative atte a sviluppare forme sinergiche di intervento nella materia della sicurezza urbana, mediante la condivisione, da parte della Tenenza, delle immagini della videosorveglianza già installate nel territorio Comunale;
- Il Comune, in qualità di Titolare del trattamento dati, si rende disponibile a nominare mediante la presente convenzione il Comandante della Stazione quale Responsabile esterno del trattamento dei dati, lo stesso potrà successivamente individuare, previa comunicazione al Comune, una persona fisica incarica o comunque un numero limitato di persone nell'ambito dei carabinieri dell'Arma, nei casi in cui risulta indispensabile per le finalità perseguite alla visione delle registrazioni;
- Le Parti si impegnano a intensificare il rapporto di collaborazione anche tramite il Corpo di Polizia Locale secondo le modalità e i limiti previsti dalle normative vigenti e in relazione alle proprie competenze;

Visti i contenuti del Regolamento Europeo sulla protezione dei dati personali 679/2016 e il Codice nazione sulla privacy dlga 196/2003;

Tra il Comune di _____ e la Stazione dei Carabinieri di _____, rappresentati rispettivamente dal Sindaco e dal Comandante, si conviene quanto segue:

1) Il Comune in qualità di Titolare del trattamento dei dati concede alla Stazione dei Carabinieri l'accesso alle proprie telecamere per la videosorveglianza sul territorio comunale alle seguenti condizioni:
   a) Il Comandante della Stazione Carabinieri è nominato Responsabile esterno del trattamento dei dati, il quale dovrà rispettare quanto previsto in tema di trattamento dei dati personali dalla normativa vigente;
   b) L'accesso al sistema di videosorveglianza avviene tramite un unico account dedicato e personalizzato sul sistema informatico dedicato, il cui funzionamento è gestito dai servizi informatici del Comune ed è tracciato;
   c) Nessun soggetto è autorizzato ad accedere fisicamente agli impianti di videosorveglianza se non preventivamente autorizzato dal Titolare;
   d) Il Responsabile esterno del trattamento dei dati è l'unico soggetto autorizzato all'accesso delle immagini, custodisce le password per l'utilizzo dei sistemi e cura il rispetto dei requisiti di sicurezza sia informatici che fisici delle proprie postazioni informatiche che accedono al sistemi di videosorveglianza;
   e) Il Responsabile può nominare, previa comunicazione al Comune, una persona fisica espressamente incaricata del trattamento dei dati o comunque un numero limitato di persone nell'ambito dei carabinieri dell'Arma, dell'accesso al sistema e nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni. Lo stesso

Responsabile del trattamento, tramite visite periodiche, vigilerà sull'attività degli incaricati in relazione alle istruzioni impartite e alla puntuale osservanza delle disposizioni normative e regolamentari;

f) Il Responsabile comunicherà tempestivamente qualsiasi criticità dovesse riscontrare nell'uso degli impianti di videosorveglianza;

Per tutto ciò che non viene espressamente menzionato nella presente convenzione, si dovrà fare riferimento a quanto previsto nel Regolamento Comunale per la Videosorveglianza e Fototrappolaggio che risulta pubblicato sul sito web ufficiale del Comune, alla normativa vigente nonché agli orientamenti applicativi del Garante per la privacy.

La presente convenzione ha durata triennale salvo rinnovo.

_____lì, _____

Il Sindaco di _____

_____

Il Comandante della Stazione di _____

_____

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	**REGISTRO UNICO DEI TRATTAMENTI (Art. 30 c. 1 e 2 del Regolamento 679/2016/UE – GDPR)**																		
2	**ENTE TITOLARE DEL TRATTAMENTO**	**COMUNE DI _____**	**Responsabile protezione dati**		**Delegato dal Titolare (eventuale)**	**_____**	**Registro tenuto da**												
3	Indirizzo		Indirizzo		Indirizzo		Data di creazione												
4	N.telefono		N.telefono		N.telefono		Ultimo aggiornamento												
5	Mail		Mail		Mail		N. schede compilate												
6	PEC		PEC		PEC		Prossima revisione												
7																			
8	**NUMERAZIONE**	**TRATTAMENTO**						**DATI PERSONALI**			**INTERESSATI**		**DESTINATARI**		**TRASFERIMENTI**	**SICUREZZA**	**REGISTRO**		**INCARICATI**
9	**n.ordine**	**Descrizione**	**Finalità**	**Categorie**	**Contitolare (eventuale)**	**Designato (responsabile interno)**	**Reponsabile esterno (eventuale)**	**Categoria**	**Dati Sensibili (SI/NO)**	**Termine Ultimo cancellazione**	**Categoria**	**Consenso (SI/NO)**	**Categoria**	**Paesi Terzi - Organi Internazionali (eventuale) (SI/NO)**	**Paesi Terzi - Organi Internazionali (eventuale) (SI/NO)**	**Misure tecniche ed organizzative adottate**	**Digitale**	**Cartaceo**	**SI/NO**
10	*CODICE UNIVOCO (es. 001)*	*BREVE DESCRIZIONE DEL TRATTAMENTO (es. Iscrizione anagrafica; gestione dati protocollo; procedure di gara di appalto; ecc….)*	*[ ] l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (in questo caso il consenso sarà acquisito con separato atto);* *[ ] il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; Dettagli: ……* *[ ] il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; Dettagli: ……* *[ ] il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; Dettagli: ……* *[ ] il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; Dettagli: ……* *[ ] il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.*	*[ ] raccolta* *[ ] registrazione* *[ ] organizzazione* *[ ] strutturazione* *[ ] conservazione* *[ ] adattamento o modifica* *[ ] estrazione* *[ ] consultazione* *[ ] uso* *[ ] comunicazione mediante trasmissione* *[ ] diffusione o qualsiasi altra forma di messa a disposizione* *[ ] raffronto od interconnessione* *[ ] limitazione* *[ ] cancellazione o distruzione* *[ ] profilazione* *[ ] pseudonimizzazione* *[ ] ogni altra operazione applicata a dati personali Dettagli: ……*	*Dati identificativi*	*Dati identificativi (da compilare)*	*Dati identificativi (da compilare)*	*[ ] dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro) Dettagli: ……* *[ ] situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale.* *[ ] dati inerenti lo stile di vita* *[ ] situazione economica* *[ ] situazione finanziaria* *[ ] situazione patrimoniale* *[ ] situazione fiscale* *[ ] dati di connessione: indirizzo IP, login, altro.* *[ ] dati di localizzazione: ubicazione, GPS, GSM, altro.*	*[ ] Dati inerenti l'origine razziale o etnica* *[ ] opinioni politiche* *[ ] convinzioni religiose o filosofiche* *[ ] appartenenza sindacale* *[ ] salute, vita o orientamento sessuale* *[ ] dati genetici e biometrici* *[ ] dati relativi a condanne penali* *Dettagli: ……*	*Non determinabile*	*[ ] Cittadini residenti* *[ ] minori di anni 16* *[ ] elettori* *[ ] contribuenti* *[ ] utenti* *[ ] partecipanti al procedimento* *[ ] dipendenti* *[ ] amministratori* *[ ] fornitori* *[ ] altro*	*[ ] SI* *[ ] NO*	*[ ] persone fisiche* *[ ] autorita pubbliche* *[ ] ……*	*[ ] SI* *[ ] NO*	*Indicare*	*[ ] misure specifiche poste in essere per fronteggiare rischi di distruzione, perdita, modifica, accesso, divulgazione non autorizzata, la cui efficacia va valutata regolarmente* *[ ] Sistemi di autenticazione* *[ ] sistemi di autorizzazione* *[ ] sistemi di protezione (antivirus; firewall; antintrusione; altro) adottati per il trattamento* *[ ] Sicurezza anche logistica*	*[ ] SI* *[ ] NO*	*[ ] SI* *[ ] NO*	*[ ] SI* *[ ] NO*
11	1	Servizi istituzionali, generali e di gestione	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
12	2	Organi istituzionali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
13	3	Segreteria generale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
14	4	Gestione economica, finanziaria, programmazione, provveditorato	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione economica, situazione finanziaria, situazione patrimoniale, situazione fiscale;	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
15	5	Gestione delle entrate tributarie e servizi fiscali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione economica, situazione finanziaria, situazione patrimoniale, situazione fiscale;	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
16	6	Gestione dei beni demaniali e patrimoniali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
17	7	Ufficio tecnico	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
18	8	Elezioni e consultazioni popolari - Anagrafe e stato civile	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, culturale, sociale;	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
19	9	Statistica e sistemi informativi	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro) dati di connessione: indirizzo IP, login, altro, dati di localizzazione: ubicazione, GPS, GSM, altro;	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
20	10	Assistenza tecnico-amministrativa agli enti locali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
21	11	Risorse umane	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro) Dettagli: situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale. Dati inerenti lo stile di vita, situazione economica, situazione finanziaria, situazione patrimoniale, situazione fiscale, dati di connessione: indirizzo IP, login, altro.	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
22	12	Altri servizi generali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
23	13	Giustizia	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
24	14	Uffici giudiziari	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
25	15	Casa circondariale e altri servizi	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
26	16	Ordine pubblico e sicurezza	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
27	17	Polizia locale e amministrativa	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
28	18	Sistema integrato di sicurezza urbana	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
29	19	Istruzione e diritto allo studio	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro) Dettagli: situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale. Dati inerenti lo stile di vita, situazione economica, situazione finanziaria, situazione patrimoniale, situazione fiscale, dati di connessione: indirizzo IP, login, altro.	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
30	20	Istruzione prescolastica	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro) Dettagli: situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale. Dati inerenti lo stile di vita, situazione economica, situazione finanziaria, situazione patrimoniale, situazione fiscale, dati di connessione: indirizzo IP, login, altro.	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
31	21	Altri ordini di istruzione non universitaria[i]	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
32	22	Istruzione universitaria	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
33	23	Istruzione tecnica superiore	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
34	24	Servizi ausiliari all'istruzione	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
35	25	Tutela e valorizzazione dei beni e delle attività culturali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
36	26	Valorizzazione dei beni di interesse storico	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
37	27	Attività culturali e interventi diversi nel settore culturale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
38	28	Politiche giovanili, sport e tempo libero	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
39	29	Sport e tempo libero	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
40	30	Giovani	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
41	31	Turismo	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
42	32	Sviluppo e la valorizzazione del turismo	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
43	33	Assetto del territorio ed edilizia abitativa	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
44	34	Urbanistica e assetto del territorio	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
45	35	Edilizia residenziale pubblica e locale e piani di edilizia economico-popolare	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
46	36	Sviluppo sostenibile e tutela del territorio e dell'ambiente	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
47	37	Difesa del suolo	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
48	38	Tutela, valorizzazione e recupero ambientale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
49	39	Rifiuti	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
50	40	Servizio idrico integrato	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
51	41	Aree protette, parchi naturali, protezione naturalistica e forestazione	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
52	42	Tutela e valorizzazione delle risorse idriche	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
53	43	Sviluppo sostenibile territorio montano piccoli Comuni	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
54	44	Qualità dell'aria e riduzione dell'inquinamento	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
55	45	Trasporti e diritto alla mobilità	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
56	46	Trasporto ferroviario	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
57	47	Trasporto pubblico locale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
58	48	Trasporto per vie d'acqua	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
59	49	Altre modalità di trasporto	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
60	50	Viabilità e infrastrutture stradali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
61	51	Soccorso civile	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
62	52	Sistema di protezione civile	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
63	53	Interventi a seguito di calamità naturali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
64	54	Diritti sociali, politiche sociali e famiglia	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
65	55	Interventi per l'infanzia e i minori e per asili nido	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
66	56	Interventi per la disabilità	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
67	57	Interventi per gli anziani	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
68	58	Interventi per i soggetti a rischio di esclusione sociale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
69	59	Interventi per le famiglie	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
70	60	Interventi per il diritto alla casa	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale;	SI	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
71	61	Programmazione e governo della rete dei servizi sociosanitari e sociali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
72	62	Cooperazione e associazionismo	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
73	63	Servizio necroscopico e cimiteriale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
74	64	Tutela della salute	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
75	65	Ulteriori spese in materia sanitaria	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
76	66	Sviluppo economico e competitività	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
77	67	Industria, PMI e Artigianato	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
78	68	Commercio - reti distributive - tutela dei consumatori	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
79	69	Ricerca e innovazione	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
80	70	Reti e altri servizi di pubblica utilità	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
81	71	Politiche per il lavoro e la formazione professionale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
82	72	Servizi per lo sviluppo del mercato del lavoro	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
83	73	Formazione professionale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
84	74	Sostegno all'occupazione	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
85	75	Agricoltura, politiche agroalimentari e pesca	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
86	76	Sviluppo del settore agricolo e del sistema agroalimentare	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
87	77	Caccia e pesca	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
88	78	Energia e diversificazione delle fonti energetiche	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
89	79	Fonti energetiche	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
90	80	Relazioni con le altre autonomie territoriali e locali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
91	81	Relazioni finanziarie con le altre autonomie territoriali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
92	82	Relazioni internazionali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI
93	83	Relazioni internazionali e Cooperazione allo sviluppo	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;	acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione;	NO			Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro);	NO	Non determinabile;	Cittadini residenti, utenti, fornitori, dipendenti, amministratori;	NO	Persone fisiche, autorità pubbliche;	NO	NO	Sistemi di autenticazione, di autorizzazione, di protezione (antivirus; firewall; antintrusione; altro), sicurezza anche logistica	SI	SI	SI

COMUNE DI _____

Provincia di _____

Decreto di designazione del Responsabile della Protezione dei Dati personali (RDP) ai sensi dell'art. 37 del Regolamento UE 2016/679

IL SINDACO

Premesso che:

- Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile dei dati personali (RDP) (artt. 37-39);
- Il predetto Regolamento prevede l'obbligo per il titolare o il responsabile del trattamento di designare il *RPD «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali»* (art. 37, paragrafo 1, lett a);
- Le predette disposizioni prevedono che il RPD *«può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi»* (art. 37, paragrafo 6) e deve essere individuato *«in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39»* (art. 37, paragrafo 5) *e «il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento»* (considerando n. 97 del RGPD);

Nel caso in cui si opti per la designazione di un RPD condiviso si dovrà aggiungere

- Le disposizioni prevedono inoltre che *«un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione»* (art. 37, paragrafo 3);

Considerato che *l'Ente X:*

- è tenuto alla designazione obbligatoria del RPD nei termini previsti, rientrando nella fattispecie prevista dall'art. 37, par. 1, lett a) del RGPD;

Nel caso in cui si opti per la designazione di un RPD condiviso si dovrà aggiungere

- ha ritenuto di avvalersi della facoltà, prevista dall'art. 37, paragrafo 3, del Regolamento, di procedere alla nomina condivisa di uno stesso RPD con gli *Enti X, Y, Z,* sulla base delle valutazioni condotte di concerto con i predetti Enti in ordine a … (es. dimensioni, affinità tra le relative strutture organizzative, funzioni (attività) e trattamenti di dati personali, razionalizzazione della spesa);

- all'esito di … (*indicare la procedura selettiva interna o esterna, gara, altro*) ha ritenuto che il la/il ……., sia in possesso del livello di conoscenza specialistica e delle competenze richieste dall'art. 37, par. 5, del RGPD, per la nomina a RPD, e non si trova in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare;

Il predetto, nel rispetto di quanto previsto dall'art. 39, par. 1, del RGPD è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

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 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 d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 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'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

(*è possibile inserire di seguito anche ulteriori compiti, purché non incompatibili, quali ad es.:*

f) tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile ed attenendosi alle istruzioni impartite…)

I compiti del Responsabile della Protezione dei Dati personali attengono all'insieme dei trattamenti di dati effettuati dall' Ente X.

L'*Ente X* si impegna a:

a) mettere a disposizione del RPD le seguenti risorse al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate … (*specificare, ad es. se è stato istituito un apposito Ufficio o gruppo di lavoro, le relative dotazioni logistiche e di risorse umane, nonché i compiti o le responsabilità individuali del personale*);
b) non rimuovere o penalizzare il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;

c) garantire che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse;

DECRETA

Di designare …… come Responsabile dei dati personali (RPD) per *l'Ente X*

Data ……..

Il nominativo e i dati di contatto del RPD (recapito postale, telefono, email) saranno resi disponibili nella intranet dell'Ente (url…., ovvero bacheca) e comunicati al Garante per la protezione dei dati personali. I dati di contatto saranno, altresì, pubblicati sul sito internet istituzionale.

COMUNE DI _____

Provincia di _____

DECRETO DI NOMINA DEL DESIGNATO AL TRATTAMENTO DEI DATI PERSONALI

IL SINDACO

Visto il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), più avanti sintetizzato come Regolamento;

Visto il dlgs 196/2003 aggiornato dal dlgs 101/2018;

Visto il Regolamento di Organizzazione degli Uffici e dei Servizi approvato con d.g. n. ___ del _____ come integrato con d.g. n. _____ del _____;

Visto il Regolamento in tema di protezione dei dati personali approvato con d.g. n. _____ del _____;

Premesso che:

1. Il Sindaco pro tempore ricopre il ruolo di titolare del trattamento dei dati in rappresentanza dell'Ente;
2. Il titolare del trattamento dei dati svolge una attività che comporta il trattamento di dati personali;
3. Il medesimo, tenendo 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, ha ritenuto di conseguenza mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento viene e sarà costantemente effettuato uniformandosi ai principi contenuti nel regolamento sopra citato;
4. Le relative soluzioni tecniche ed organizzative richiedono una costante monitoraggio e puntuale anche mediante riesami e periodici aggiornamenti;
5. Tali misure devono tenere conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso;
6. Il titolare del trattamento sa di essere tenuto anche a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati, quali la pseudonimizzazione e la minimizzazione;
7. Il titolare del trattamento è altresì consapevole di dovere anche integrare, nel trattamento, le necessarie garanzie al fine di soddisfare i requisiti del suddetto regolamento e tutelare i diritti degli interessati alla riservatezza e adeguato trattamento dei dati personali;
8. Il titolare del trattamento è consapevole di essere tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, tali obblighi valgono per

la quantità dei dati personali raccolti, per la portata del trattamento ed anche per il periodo di conservazione e l'accessibilità, dette misure devono garantire che, per impostazione predefinita, non siano resi accessibili dati personali ad un numero indefinito di persone fisiche ma esclusivamente a coloro che ne siano autorizzati;

9. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità;
10. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta;
11. Il soggetto indicato come designato al trattamento dei dati (responsabile interno) deve essere adeguatamente formato ed edotto di tutti gli obblighi che incombono sul titolare del trattamento e si impegna a rispettarne e consentirne ogni prerogativa, obbligo, onere e diritto che discende da tale posizione giuridica;
12. Il designato al trattamento si impegna ad informare il titolare del trattamento di eventuali modifiche previste al processo di trattamento dei dati e riguardanti l'aggiunta o la sostituzione di altri responsabili (esterni) del trattamento, dando così al titolare l'opportunità d'intervenire;
13. Il designato al trattamento è tenuto a trattare i dati personali su istruzione documentata del titolare del trattamento, ai sensi di legge e dei regolamenti dell'Ente;
14. Il designato al trattamento garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
15. Il designato al trattamento assicura che procederà alla pseudonimizzazione ed alla cifratura dei dati personali quando necessario;
16. Il designato al trattamento garantisce di avere la capacità strutturale, tecnica ed organizzativa di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
17. Il designato al trattamento si impegna ad adottare tutte le misure richieste per la sicurezza del trattamento dei dati;
18. Il designato al trattamento è tenuto ad assistere il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del regolamento. Tale obbligo di assistenza riguarda anche la garanzia del rispetto, da parte del titolare del trattamento, degli obblighi di cui agli articoli da 32 a 36 del regolamento. Il tutto tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento. Per tale obblighi di assistenza si terrà conto della natura del trattamento;
19. Il designato al trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi specificati ed inoltre consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato;
20. Nel caso in cui il designato al trattamento ritenga che, a suo avviso, una delle istruzioni violi il regolamento o altre disposizioni nazionali o dell'unione riguardo al trattamento dei dati personali, ne informa immediatamente il titolare del trattamento;

21. Il designato al trattamento si impegnano a far sì che, chiunque agisca sotto la sua autorità e abbia accesso a dati personali, non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri;
22. In caso di violazione dei dati, tale da presentare un rischio per i diritti e le libertà fondamentali delle persone, il designato al trattamento si dichiara consapevole degli obblighi che incombono sul titolare del trattamento a norma dell'art. 33 del regolamento. Di conseguenza si impegna a comunicare ogni circostanza e dato rilevane, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione, il titolare del trattamento;
23. Il titolare del trattamento e il designato al trattamento si impegnano ad assicurare che il responsabile della protezione dei dati sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
24. Il titolare del trattamento e il designato al trattamento si impegnano a sostenere il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 del regolamento fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti nonché per mantenere la propria conoscenza specialistica;
25. E' fatto obbligo al designato al trattamento attenersi alle indicazioni fornite dal responsabile della protezione dei dati e di rendersi disponibile per ogni campagna di sensibilizzazione e formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
26. Se richiesto, il designato al trattamento dei dati è tenuto a fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del regolamento, a cooperare con l'autorità di controllo e a fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

DECRETA

1. Ai sensi dell'art. 2 c. quaterdecies del dlgs 196/2003 di nominare _____, dirigente/responsabile titolare di posizione organizzativa della struttura _____, in possesso dei requisiti di esperienza, capacità ed affidabilità, quale Designato al trattamento dei dati (Responsabile interno);
2. Di delegare dirigente/responsabile come sopra individuato l'esercizio della rappresentanza dell'Ente, in qualità di designato al trattamento dei dati personali, realizzati nell'ambito dell'incarico conferito e dell'inquadramento organizzativo a cui questo è preposto;
3. Di dare pubblicità del presente atto tramite la pubblicazione dello stesso all'Albo pretorio on line e l'inserimento all'interno del sito istituzionale dell'Ente, nel Link "Amministrazione Trasparente";
4. Di notificare copia del presente decreto all'interessato;
5. Di dare l'immediata eseguibilità al presente atto al fine di procedere ai successivi adempimenti ivi richiamati.

COMUNE DI _____

Provincia di _____

Al Professionista/Società _____
pec: _____

OGGETTO: COMUNICAZIONE AL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Visto il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), più avanti sintetizzato come Regolamento;

Visto il dlgs 196/2003 aggiornato dal dlgs 101/2018;

Visto il Regolamento di Organizzazione degli Uffici e dei Servizi approvato con d.g. n. ___ del _____ come integrato con d.g. n. _____ del _____;

Visto il Regolamento in tema di protezione dei dati personali approvato con d.g. n. _____ del _____;

In qualità di Titolare del trattamento dei dati personali, Sindaco pro tempore dell'Ente, nell'ambito dell'appalto di servizi che svolge per questo Ente sulla base di specifcio rapporto contrattuale in essere, si comunica che è incaricato di svolge il ruolo di Responsabile del trattamento dei dati personali (esterno) e che risulta soggetto a tutti gli obblighi, oneri, doveri e prerogative previste dalla normativa vigente;

Nel dettaglio si rappresenta che:

1. Il titolare del trattamento dei dati svolge una attività che comporta il trattamento di dati personali;
2. Il medesimo, tenendo 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, ha ritenuto di valutare i rischi e, di conseguenza, mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento viene e sarà costantemente effettuato uniformandosi al regolamento sopra citato;
3. Le relative soluzioni tecniche ed organizzative richiedono una costante monitorizzazione anche mediante riesami e periodici aggiornamenti;
4. Tali misure devono tenere conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso;

5. Il titolare del trattamento sa di essere tenuto anche a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati, quali la pseudonimizzazione e la minimizzazione;
6. Il titolare del trattamento è altresì consapevole di dovere anche integrare, nel trattamento, le necessarie garanzie al fine di soddisfare i requisiti del suddetto regolamento e tutelare i diritti degli interessati alla riservatezza ed adeguato trattamento dei dati personali;
7. Il titolare del trattamento è consapevole di essere tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tali obblighi valgono per la quantità dei dati personali raccolti, per la portata del trattamento ed anche per il periodo di conservazione e l'accessibilità, dette misure devono garantire che, per impostazione predefinita, non siano resi accessibili dati personali ad un numero indefinito di persone fisiche senza l'intervento della persona fisica;
8. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato;
9. Il soggetto indicato come responsabile del trattamento deve essere edotto di tutti gli obblighi che incombono sul titolare del trattamento e si impegna a rispettarne e consentirne ogni prerogativa, obbligo, onere e diritto che discende da tale posizione giuridica;
10. Il responsabile del trattamento si impegna ad informare il titolare del trattamento di eventuali modifiche previste al processo di trattamento riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento (sub responsabili), dando così al titolare l'opportunità di opporsi a tali modifiche;
11. Il responsabile del trattamento è tenuto a trattare i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. Il responsabile del trattamento in tal caso è tenuto ad informare il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
12. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
13. Il responsabile del trattamento assicura che procederà alla pseudonimizzazione ed alla cifratura dei dati personali;
14. Il responsabile del trattamento garantisce di avere la capacità strutturale, tecnica ed organizzativa di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
15. Il responsabile del trattamento si impegna ad adottare tutte le misure richieste dall'art. 32 ed a rispettare le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 del Regolamento;
16. Il responsabile del trattamento è tenuto ad assistere il titolare del trattamento, unicamente per le attività di sua competenza, con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento. Tale obbligo di assistenza riguarda anche la garanzia del rispetto, da parte

del titolare del trattamento, degli obblighi di cui agli articoli da 32 a 36 del Regolamento. Il tutto tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento. Per tali obblighi di assistenza si terrà conto della natura del trattamento;

17. Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi specificati ed inoltre consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato;
18. Nel caso in cui il responsabile del trattamento ritenga che, a suo avviso, una delle istruzioni violi il regolamento o altre disposizioni nazionali o dell'unione riguardo al trattamento dei dati personali, informa immediatamente il responsabile della protezione dei dati (DPO - data Protection Officer – art. lo 37 del regolamento);
19. Il responsabile del trattamento si impegna a far sì che, chiunque agisca sotto la sua autorità e abbia accesso a dati personali, non tratti tali dati se non è istruito in tal senso, salvo che lo richieda il diritto dell'Unione o degli Stati membri;
20. In caso di violazione dei dati, tale da presentare un rischio per i diritti e le libertà fondamentali delle persone, il responsabile del trattamento si dichiara consapevole degli obblighi che incombono sul titolare del trattamento a norma dell'art. 33 del regolamento. Di conseguenza si impegna a comunicare ogni circostanza e dato rilevane, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione, il titolare del trattamento. A tale fine di ricorda che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo;
21. Se richiesto, il responsabile del trattamento dei dati è tenuto a fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del regolamento, a cooperare con l'autorità di controllo ed a fungere da punto di contatto per l'autorità di controllo 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;

Riservandoci di fornire ulteriori istruzioni e comunicazioni in merito, rimaniamo a disposizione per ogni eventuale chiarimento o richiesta.

_____, lì_____

Il Sindaco, Titolare del Trattamento

_____

Per accettazione
Il Legale Rappresentante

_____

INFORMATIVA SULLA PRIVACY AI SENSI DEL DGPR 679/2016 E DEL DLGS 196/2003

In ottemperanza degli obblighi in materia di trattamento dei dati personali derivanti dal Regolamento europeo per la protezione dei dati personali n. 679/2016 GDPR, dalla normativa nazionale dlgs 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali, aggiornato al dlgs 101/2018 e s.m.i., si informa che i dati personali forniti formeranno oggetto di trattamento nel rispetto della normativa sopra richiamata e degli obblighi di riservatezza.

Lo scopo della presente informativa estesa sulla privacy, ai sensi dell'art. 13 del Regolamento UE 679/2016, è di fornire la massima trasparenza relativamente alle informazioni che verranno acquisite sia in formato elettronico che cartaceo e come vengono usate.

1. **Titolare del trattamento**

Il Titolare e responsabile dei dati raccolti è _____, rappresentato da _____ per il ruolo di _____ protempore, con sede legale in _____. Per chiedere informazioni relative ai suoi dati personali o l'aggiornamento o la cancellazione degli stessi e in generale per l'esercizio dei diritti e delle facoltà sopra descritti, l'utente dovrà farne richiesta espressa diretta al titolare del trattamento con qualunque mezzo che consenta di documentare l'avvenuto invio e la ricezione della richiesta di cui sopra che conterrà le seguenti informazioni, Rif.: tutela dei dati personali - nome, cognome, fotocopia carta di identità, domicilio e firma dell'interessato, attraverso raccomandata all'indirizzo riportato oppure tramite posta elettronica certificata a: _____.

Il Titolare del trattamento può nominare uno o più Responsabili del trattamento dei dati individuati tra il personale interno che possegga adeguate competenze manageriali e ricopra ruoli di responsabilità.

Il Titolare del trattamento può nominare uno o più Corresponsabili del trattamento dei dati individuati tra le persone fisiche o giuridiche esterne che gestiscano servizi per suo conto e quindi trattino dati personali, in ragione di specifici accordi contrattuali.

2. **Responsabile della protezione dei dati (DPO)**

Il Responsabile della protezione dei dati (DPO) è _____ con sede in _____, i contatti e i riferimenti del DPO sono email: _____ posta elettronica certificata: _____.

3. **Dati trattati, finalità e basi giuridiche del trattamento**

I dati personali forniti sono necessari per gli adempimenti previsti per legge, incluse le opportune e necessarie comunicazioni necessarie allo svolgimento dei servizi istituzionali offerti.

I dati personali forniti dall'utente tramite form di registrazione, domande o contratti sono raccolti e trattati per le seguenti finalità:

1. Al trattamento dei dati personali inclusi quelli considerati come categorie particolari di dati (dati sensibili) per i soli fini istituzionali o legati al servizio in oggetto;
2. Al trattamento dei dati personali anche per attività di comunicazione diretta e marketing strettamente connessi ai servizi erogati;
3. Alla comunicazione (eventuale) dei dati personali ad altre pubbliche amministrazioni, professionisti o società di natura privata nei soli casi previsti da una norma di legge, regolamento o contratto.

La base giuridica che legittima il trattamento è l'art. 6 c. 1 lett. e) del Regolamento UE 679/2016, ovvero il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare per il trattamento interno dei dati ai fini della erogazione dei servizi istituzionali.

Tenuto conto delle finalità del trattamento come sopra illustrate, il conferimento dei dati strettamente necessari all'erogazione dei servizi è obbligatorio e il loro mancato, parziale o inesatto conferimento potrà avere come conseguenza l'impossibilità di svolgere l'attività prevista.

4. **Modalità di trattamento e conservazione**

Il trattamento sarà svolto in forma automatizzata e/o manuale, nel rispetto di quanto previsto dall'art. 32 del GDPR 2016/679 ad opera di soggetti appositamente incaricati e in ottemperanza a quanto previsto dagli art. 29 GDPR 2016/679.

Nel rispetto dei principi di liceità, limitazione delle finalità e minimizzazione dei dati, ai sensi dell'art. 5 GDPR 2016/679, i dati personali saranno conservati per il periodo di tempo necessario per il conseguimento delle finalità per le quali sono raccolti e trattati, salvo richiesta di cancellazione da parte dell'interessato se possibile.

I dati forniti volontariamente dall'utente verranno trattati con sistemi manuali ed automatizzati, verranno registrati su supporti informatici protetti e se anche in moduli cartacei, correttamente mantenuti e protetti secondo modalità e con strumenti idonei a garantire la sicurezza e la riservatezza dei dati stessi, in conformità di quanto previsto dalla normativa.

I dati "sensibili" eventualmente trattati saranno resi anonimi e conservati con particolari disposizioni di sicurezza.

I trattamenti dei dati personali raccolti tramite questo sito internet e forniti volontariamente dall'utente hanno luogo presso le sedi del titolare del trattamento e dei soggetti direttamente collegati, sono curati altresì solo da personale incaricato del trattamento. Il trattamento e la conservazione dei dati di navigazione avvengono su server ubicati all'interno dell'Unione Europea, anche presso società terze professionali incaricate e debitamente nominate quali Responsabili del Trattamento. I dati non sono trasferiti fuori dall'Unione Europea. Il Titolare si riserva la facoltà di modificare l'ubicazione dei server anche fuori dall'Unione Europea, assicurando, in tal caso, che il trasferimento avverrà in conformità alle disposizioni di legge applicabili, con le adeguate garanzie previste dall'art. 46 del Regolamento UE 679/2016.

5. Soggetti autorizzati al trattamento, responsabili e comunicazione dei dati

Il trattamento dei dati raccolti è effettuato da personale interno a tal fine individuato e autorizzato del trattamento secondo specifiche istruzioni impartite nel rispetto della normativa vigente. Informiamo inoltre che i dati raccolti non saranno mai diffusi e non saranno oggetto di comunicazione, salvo le comunicazioni necessarie che possono comportare il trasferimento di dati ad enti pubblici, a società, consulenti o ad altri soggetti strettamente legati per l'adempimento di attività istituzionali, degli obblighi di legge, regolamentari o a fini statistici.

6. Pubblicazione dei dati

I dati acquisiti vengono pubblicati solo ed esclusivamente, nella modalità e relativa tempistica, se previsto da una disposizione di legge.

7. A quali soggetti saranno comunicati i dati raccolti

I dati potranno essere comunicati al fine di conseguire l'adempimento della sua richiesta, degli obblighi contrattuali e/o di legge:

1. A tutti i soggetti cui la facoltà di accesso a tali dati è riconosciuta in forza di provvedimenti normativi;
2. Ai collaboratori e dipendenti interni nell'ambito esclusivamente delle relative mansioni istituzionali e se preventivamente autorizzati;
3. Ai collaboratori, partner e a società o professionisti esterni debitamente nominati come responsabili del trattamento.

8. Trasferimento dei dati personali

I suoi dati non saranno trasferiti né in Stati membri dell'Unione Europea né in Paesi terzi non appartenenti all'Unione Europea.

9. Minori

Se l'Interessato ha meno di 14 anni, fermo restando quanto sopra previsto, il trattamento è lecito soltanto se e nella misura in cui il consenso, se dovuto, è prestato o autorizzato dal titolare della responsabilità genitoriale per il quale devono essere acquisiti i dati identificativi e copia dei documenti di riconoscimento.

10. Diritti dell'interessato

In ogni momento, si potranno esercitare, ai sensi degli articoli dal 15 al 22 del Regolamento UE n. 2016/679, il diritto di:

1. Chiedere la conferma dell'esistenza o meno di propri dati personali;
2. Ottenere le indicazioni circa le finalità del trattamento, le categorie dei dati personali, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e, quando possibile, il periodo di conservazione;
3. Ottenere la rettifica e la cancellazione dei dati, se possibile;
4. Ottenere la limitazione del trattamento;

5. Ottenere la portabilità dei dati, ossia riceverli da un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico e trasmetterli ad un altro titolare del trattamento senza impedimenti;
6. Opporsi al trattamento in qualsiasi momento ed anche nel caso di trattamento per finalità di comunicazioni dirette;
7. Opporsi ad un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione.
8. Revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
9. Proporre reclamo all'autorità di controllo.

Può esercitare i Suoi diritti con richiesta scritta inviata a mezzo raccomandata all'indirizzo postale della sede legale o all'indirizzo di posta elettronica certificata: _____.

11. Tipologia dei dati trattati nell'ambito della navigazione sul sito web ufficiale

I sistemi informatici e le procedure software preposte al funzionamento di questo sito acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nei protocolli di comunicazione di Internet. Si tratta di informazioni che non sono raccolte per essere associate agli interessati identificati ma che per la loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. Questi dati potrebbero essere utilizzati per l'accertamento di eventuali responsabilità in caso di ipotetici reati informatici ai danni del sito o comunque connessi alla navigazione su eventuali link.

In questa categoria di dati rientrano:

1. Indirizzi IP;
2. Nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito;
3. Indirizzi di notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, metodo utilizzato nel sottoporre la richiesta al server, dimensione del file ottenuto in risposta, codice numerico indicante lo stato della risposta data dal server (buon fine, errore, etc.) ed altri parametri relativi al sistema operativo ed all'ambiente informatico dell'utente;
4. Dati forniti volontariamente dall'utente: quelli inviati facoltativamente, in forma esplicita e volontaria inviati tramite form di contatto, form di registrazione, nonché per particolari servizi a domanda.

12. Informativa estesa sull'uso dei cookie

Questo sito utilizza i Cookie per rendere i propri servizi semplici ed efficienti.
Gli utenti che visionano il Sito, vedranno inserite delle quantità minime di informazioni nei dispositivi in uso, che siano computer e periferiche mobili, in piccoli file di testo denominati "cookie" salvati nelle directory utilizzate dal browser web dell'Utente. Disabilitando i cookie alcuni dei nostri servizi o pagine potrebbero non essere utilizzabili o non funzionare correttamente. Vi sono vari tipi di cookie, alcuni necessari per rendere più efficace l'uso del Sito, altri per abilitare determinate funzionalità. Analizzandoli in maniera particolareggiata i nostri cookie permettono di:

a. memorizzare le preferenze inserite;
b. evitare di reinserire le stesse informazioni piu volte durante la visita quali ad esempio nome utente e password;
c. analizzare l'utilizzo dei servizi e dei contenuti forniti dal sito per ottimizzarne l'esperienza di navigazione e i servizi offerti, per finalità statistiche.

Tipologie di Cookie utilizzati da questo sito: a seguire i vari tipi di cookie utilizzati da questo sito in funzione delle finalità d'uso.
Cookie Tecnici:
Questa tipologia di cookie è strettamente necessaria al corretto funzionamento di alcune sezioni del Sito e non richiedono un consenso espresso per il loro utilizzo. In questa tipologia di Cookies sono ricompresi due categorie, ovvero persistenti e di sessione:

a. persistenti: una volta chiuso il browser non vengono distrutti ma rimangono fino ad una data di scadenza preimpostata;
b. di sessione: vengono distrutti ogni volta che il browser viene chiuso.

Questi cookie, inviati sempre dal nostro dominio, sono necessari a visualizzare correttamente il sito e in relazione ai servizi tecnici offerti, verranno quindi sempre utilizzati e inviati, a meno che l'utenza non modifichi le impostazioni nel proprio browser (inficiando così la visualizzazione delle pagine del sito).

Cookie analitici:

I cookie in questa categoria vengono utilizzati per collezionare informazioni sull'uso del sito. Questo sito, se non viene dato il consenso all'accettazione dei cookie, userà queste informazioni in merito ad analisi statistiche ANONIME al fine di migliorare l'utilizzo del Sito e per rendere i contenuti piu interessanti e attinenti ai desideri dell'utenza. Questa tipologia di Cookie, se non viene espresso il consenso, raccoglie dati in FORMA ANONIMA e ed esclusivamente aggregati sull'attività dell'utenza (pagine visitate, tempo di permanenza, origini del traffico di provenienza, provenienza geografica, età, genere e interessi) e su come è arrivata sul Sito. I cookie analitici sono inviati dal Sito Stesso o da domini di terze parti.
Dato che i cookie analitici sono configurati di default per anonimizzare l'indirizzo IP degli utenti, vengono considerati Cookie Tecnici per i quali non è richiesto il consenso esplicito.
Questo sito utilizza di default i cookies di Google Analitics con IP anonimizzato (Google Inc.)
Accesso alle informazioni della Terza Parte:

a. Privacy Policy: http://www.google.com/policies/privacy/
b. Cookie Policy: https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage
c. Disattivazione: https://tools.google.com/dlpage/gaoptout?hl=it

Cookie per integrare prodotti e funzioni di software di terze parti:
Questa tipologia di cookie integra funzionalità sviluppate da terzi all'interno delle pagine del Sito come le icone e le preferenze espresse nei social network al fine di condivisione dei contenuti del sito o per l'uso di servizi software di terze parti (come i software per generare le mappe e ulteriori software che offrono servizi aggiuntivi). Questi cookie sono inviati da domini di terze parti e da siti partner che offrono le loro funzionalità tra le pagine del Sito.
QUESTO SITO NON INSTALLA COOKIE DI TERZE PARTI.

Cookie di profilazione:
Sono quei cookie necessari a creare profili utenti al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente all'interno delle pagine del Sito. NEL NOSTRO SITO NON UTILIZZIAMO COOKIE DI PROFILAZIONE NÉ NOSTRI NÉ DI TERZA PARTE.

Cookie per cui è richiesto il consenso:
Tutti i cookie diversi da quelli tecnici e analitici sopra indicati vengono installati o attivati solo a seguito del consenso espresso dall'utente la prima volta che visita il sito. Il consenso può essere espresso interagendo con il banner di informativa breve presente su tutte le pagine del sito, cliccando sul tasto CONSENTI, oppure può essere fornito o negato in maniera selettiva, secondo le modalità di seguito indicate. Di questo consenso viene tenuta traccia in occasione delle visite successive. Tuttavia, l'utente ha sempre la possibilità di revocare in tutto o in parte il consenso già espresso.
Questo sito, secondo la normativa vigente, non è tenuto a chiedere consenso per i cookie tecnici, in quanto necessari a fornire i servizi richiesti.
Per tutte le altre tipologie di cookie il consenso può essere negato dall'Utente con una o più di una delle seguenti modalità:

a. Mediante specifiche configurazioni del browser utilizzato o dei relativi programmi informatici utilizzati per navigare le pagine che compongono il Sito;
b. Mediante modifica delle impostazioni nell'uso dei servizi di terze parti.

Entrambe queste soluzioni potrebbero impedire all'utente di utilizzare o visualizzare parti del Sito.
Siti Web e servizi di terze parti
Il Sito potrebbe contenere collegamenti ad altri siti Web che dispongono di una propria informativa sulla privacy che può essere diverse da quella adottata da questo sito e che quindi non risponde di questi siti.

Come disabilitare i cookie mediante configurazione del browser.
Chrome:

1. Eseguire il Browser Chrome
2. Fare click sul menu presente nella barra degli strumenti del browser a fianco della finestra di inserimento url per la navigazione
3. Selezionare Impostazioni
4. Fare clic su Mostra Impostazioni Avanzate
5. Nella sezione "Privacy" fare clic su bottone "Impostazioni contenuti"
6. Nella sezione "Cookie" e possibile modificare le seguenti impostazioni relative ai cookie:
    - Consentire il salvataggio dei dati in locale
    - Modificare i dati locali solo fino alla chiusura del browser
    - Impedire ai siti di impostare i cookie

- Bloccare i cookie di terze parti e i dati dei siti
- Gestire le eccezioni per alcuni siti internet
- Eliminazione di uno o tutti i cookie

Per maggiori informazioni visita la pagina dedicata.

Mozilla Firefox:

1. Eseguire il Browser Mozilla Firefox
2. Fare click sul menu presente nella barra degli strumenti del browser a fianco della finestra di inserimento url per la navigazione
3. Selezionare Opzioni
4. Seleziona il pannello Privacy
5. Fare clic su Mostra Impostazioni Avanzate
6. Nella sezione "Privacy" fare clic su bottone "Impostazioni contenuti"
7. Nella sezione "Tracciamento" e possibile modificare le seguenti impostazioni relative ai cookie:
    - Richiedi ai siti di non effettuare alcun tracciamento
    - Comunica ai siti la disponibilità ad essere tracciato
    - Non comunicare alcuna preferenza relativa al tracciamento dei dati personali
8. Dalla sezione "Cronologia" e possibile:
    - Abilitando "Utilizza impostazioni personalizzate" selezionare di accettare i cookie di terze parti (sempre, dai siti piu visitato o mai) e di conservarli per un periodo determinato (fino alla loro scadenza, alla chiusura di Firefox o di chiedere ogni volta)
    - Rimuovere i singoli cookie immagazzinati

Per maggiori informazioni visita la pagina dedicata.

Internet Explorer:

1. Eseguire il Browser Internet Explorer
2. Fare click sul pulsante Strumenti e scegliere Opzioni Internet
3. Fare click sulla scheda Privacy e nella sezione Impostazioni modificare il dispositivo di scorrimento in funzione dell'azione desiderata per i cookie:
    - Bloccare tutti i cookie
    - Consentire tutti i cookie
    - Selezione dei siti da cui ottenere cookie: spostare il cursore in una posizione intermedia in modo da non bloccare o consentire tutti i cookie, premere quindi su Siti, nella casella Indirizzo Sito Web inserire un sito internet e quindi premere su Blocca o Consenti

Per maggiori informazioni visita la pagina dedicata.

Safari 6:

1. Eseguire il Browser Safari
2. Fare click su Safari, selezionare Preferenze e premere su Privacy
3. Nella sezione *Blocca Cookie* specificare come Safari deve accettare i cookie dai siti internet.
4. Per visionare quali siti hanno immagazzinato i cookie cliccare su Dettagli

Per maggiori informazioni visita la pagina dedicata.

Safari iOS (dispositivi mobile):

1. Eseguire il Browser Safari iOS
2. Tocca su Impostazioni e poi Safari
3. Tocca su Blocca Cookie e scegli tra le varie opzioni: "Mai", "Di terze parti e inserzionisti" o "Sempre"
4. Per cancellare tutti i cookie immagazzinati da Safari, tocca su Impostazioni, poi su Safari e infine su Cancella Cookie e dati

Per maggiori informazioni visita la pagina dedicata.

Opera:

1. Eseguire il Browser Opera
2. Fare click sul Preferenze poi su Avanzate e infine su Cookie
3. Selezionare una delle seguenti opzioni:
    - Accetta tutti i cookie
    - Accetta i cookie solo dal sito che si visita: i cookie di terze parti e che vengono inviati da un dominio diverso da quello che si sta visitando verranno rifiutati

- Non accettare mai i cookie: tutti i cookie non verranno mai salvati

Per maggiori informazioni visita la pagina dedicata.

Come disabilitare i cookie di servizi di terzi:

- Servizi di Google
- Facebook
- Twitter

13. Pubblicità della presente informativa

Questa informativa è visibile mediante link in calce in tutte le pagine del sito web ai sensi dell'art. 122 del dlgs 196/2003, così come modificato dal dlgs 101/2018 e in ottemperanza al Regolamento UE 679/2016.

Esempio di dicitura da aggiungere al testo dei documenti, domande e contratti ai fini della privacy:

In ottemperanza a quanto prevede la normativa sulla privacy, Regolamento UE n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e dlgs n. 196/2003 Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento, così come aggiornato dal dlgs n. 101/2018, si informa che tutti i dati personali, compresi eventualmente i così detti “dati sensibili”, vengono acquisiti per le finalità e nell’ambito dello svolgimento dei presenti servizi, che tali dati saranno trattati unicamente dai soggetti autorizzati e per l’espletamento delle attività in oggetto in conformità a quanto previsto dalla normativa sopra richiamata, che in ogni momento possono essere esercitati i diritti sui propri dati scrivendo a questo contatto _____, che l’informativa estesa contenete tutte le informazioni previste sul trattamento dei dati personali è pubblicata e visionabile sul sito web ufficiale al link: _____.

Esempio di dicitura da aggiungere ai documenti e all'email ai fini della privacy:

In ottemperanza a quanto prevede la normativa sulla privacy, Regolamento UE n. 679/2016 e dlgs n. 196/2003 così come aggiornato dal dlgs n. 101/2018, si informa che i dati personali acquisiti nell'ambito dello svolgimento dei presenti servizi saranno trattati unicamente per le attività in oggetto e in conformità a quanto previsto dalla normativa di riferimento, in ogni momento possono essere esercitati i diritti sui propri dati scrivendo al presente indirizzo mail, l'informativa estesa sul trattamento dei dati personali è pubblicata e visionabile sul sito web ufficiale.

Informazioni sulla PIA

Nome della PIA
AMMINISTRAZIONE COMUNALE

Nome autore
Sindaco

Nome valutatore
Responsabile Protezione dei Dati

Data di creazione
11/06/2018

Nome del DPO/RPD
Carmignani Simone

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
Gli interessati sono costituiti da una moltitudine di soggetti pertanto risulta difficoltoso e praticamente impossibile richiedere il parere di tutti gli interessati, l'attività richiederebbe quindi uno sforzo sproporzionato e controproducente.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento dei dati è strettamente connesso alle finalità istituzionali e alla natura del comune che è un ente territoriale di base, dotato di un certo grado di autonomia amministrativa, dedicato agli interessi della popolazione locale. Si definisce, per le sue caratteristiche di centro abitativo nel quale si svolge la vita sociale pubblica dei suoi abitanti, l'ente locale fondamentale. Il comune è il centro della vita di relazione dell'individuo, dal momento che il suo territorio coincide quasi sempre con quello di un centro abitato (città o borgo), più le campagne circostanti, con le eventuali case sparse, ed eventuali nuclei o centri abitati strettamente interdipendenti, o che si presumono tali, con il nucleo abitativo principale che possono godere di particolari forme di partecipazione ad esempio le frazioni.
L'Amministrazione Comunale si occupa principalmente di erogare servizi alla collettività nell'ambito di pubblici poteri attribuitigli dalla legge e seguendo il pubblico interesse.

Quali sono le responsabilità connesse al trattamento?

Il titolare del trattamento è il Sindaco, i responsabili del trattamento interni sono tutti i dirigenti/posizione organizzative dell'ente, vengono nominati responsabili del trattamento esterni tutti i soggetti fisici o giuridici che trattano dati per conto del Titolare nell'ambito di un appalto di forniture, opere o servizi.

Ci sono standard applicabili al trattamento?

Al momento non sono contemplati standard da applicare direttamente al trattamento.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione economica, situazione finanziaria, situazione patrimoniale, situazione fiscale; dati di localizzazione: ubicazione, GPS, GSM, altro; elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale nonchè dati relativi al casellario giudiziale.
Possono accedere ai dati persone fisiche dipendenti o collaboratori dell'ente autorizzati e autorità pubbliche nei casi previsti dalla legge, può essere affidato il trattamento dei dati a soggetti terzi nell'ambito di un appalto di forniture, opere o servizi solo se adeguatamente disciplinato.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il ciclo di vita dei dati prevede i seguenti trattamenti: acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, trasmissione.

Quali sono le risorse di supporto ai dati?

I dati vengono conservati sia cartaceamente, ovvero sulla documentazione che viene inoltrata dagli utenti e sui documenti che vengono rilasciati dall'ente, che su supporti elettronici, ovvero computer dotati di sistema operativo standard e antivirus nonchè i server su cui sono conservati tutti i dati che possono essere gestiti anche in cloud.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Le basi legali che rendono lecito il trattamento sono:
- L'interessato ha acconsentito al trattamento dei propri dati personali per uno o più scopi specifici.
- Il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte o per l'esecuzione di misure adottate su richiesta dell'interessato prima di stipulare un contratto.
- Il trattamento è necessario per adempiere a un obbligo legale a cui è soggetto il titolare del trattamento.
- Il trattamento è necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica.
- Il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o connesso all'esercizio di pubblici poteri conferiti al titolare del trattamento.
- Il trattamento è necessario ai fini degli interessi legittimi perseguiti dal titolare del trattamento o da una terza parte, eccetto laddove prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Valutazione : Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati vengono minimizzati soprattuto con particolare attenzione nell'attività di pubblicazione nel rispetto degli obblighi di trasparenza.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati vengono aggiornati periodicamente, almeno su base annuale e incrociati con le banche dati nazionali.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati vengono conservati dall'ente a tempo indeterminato, mentre la pubblicazione degli stessi rispetta i tempi previsti di leggi.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

L'informativa sul trattamento dei dati viene sempre resa a tutti gli interessati in forma sintetica sia in modalità cartacea che telematica, è poi pubblicata l'informativa estesa sul sito web dell'ente che spiega nel dettaglio come vengono trattati i dati e i cookie.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Nei casi in cui è previsto e necessario il consenso viene acquisito esplicitamente in forma scritta, per quanto riguarda la navigazione sul sito web dell'ente il consenso viene acquisito cliccando sull'apposito pulsante che compare sulla schermata.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati possono contattare direttamente il responsabile del trattamento dei dati recandosi direttamene presso l'ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Per esercitare il diritto alla calcellazione, se possibile, gli interessati possono contattare direttamente il responsabile del trattamento dei dati recandosi direttamene presso l'ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati per esercitare il diritto di limitazione od opposizione, se possibile, possono contattare direttamente il responsabile del trattamento dei dati recandosi direttamene presso l'ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi dei responsabili del trattamento sono definiti nei singoli decreti di incarico.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati non vengono trasferiti al di fuori dell'Unione Europea.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Anonimizzazione

I dati sensibili, ovvero i particolari tipi di dati e i dati relativi al casellario giudiziale, vengono trattati in maniera riservata unicamente dal personale strettamente necessario e resi sempre completamente anonimi quando pubblicati.

Valutazione : Accettabile

Controllo degli accessi logici

Ogni operatore utilizza una postazione fisica assegnata e una postazione informatica dedicata dotata di password di accesso.

Valutazione : Accettabile

Tracciabilità

I flussi documentali avvengono tramite posta elettronica, oppure attraverso lo scambio con il gestionale interno i cui flussi sono tracciati ed identificabili.

Valutazione : Accettabile

Archiviazione

Ogni responsabile controlla l'archiviazione dei dati gestiti dall'ufficio in una cartella non condivisa su una postazione informatica protetta da password.
Gli archivi generali dell'ente sono conservati su un server dedicato il cui accesso è limitato e controllato.
Per quanto riguarda gli l'archiviazione cartacea questa avviene all'interno degli uffici che trattano i dati e viene garantito l'anonimato delle informazioni contenute, per quanto riguarda i particolari tipi di dati vengono previste delle misure di protezione ulteriori come armadietti con chiusure a chiave o casseforti.

Valutazione : Accettabile

Sicurezza dei documenti cartacei

I documenti cartacei vengono conservati dal singolo responsabile che verifica che l'ufficio li custodisca il appositi raccoglitori in modo tale che non vadano dispersi e che non siano visibili a terzi.

Valutazione : Accettabile

Minimizzazione dei dati

Vengono raccolti e conservati unicamente i dati necessari all'erogazione del servizio.

Valutazione : Accettabile

Vulnerabilità

I software vengono aggiornati costantemente e l'accesso ai dati è limitato unicamente agli operatori direttamente interessati.

Valutazione : Accettabile

Lotta contro il malware

L'anti malware è regolarmente istallato e costantemente aggiornato.

Valutazione : Accettabile

Backup

I backup vengono regolarmente effettuati.

Valutazione : Accettabile

Manutenzione

La manutenzione fisica dei dispositivi viene effettuata all'occorrenza.

Valutazione : Accettabile

Sicurezza dei canali informatici

Il firewall risulta regolarmente istallato e costantemente aggiornato.

Valutazione : Accettabile

Controllo degli accessi fisici

Gli accessi fisici agli uffici sono limitati e controllati.

Valutazione : Accettabile

Sicurezza dell'hardware

L'accesso alla rete interna è limitato, viene protetto da account e password personali.

Valutazione : Accettabile

Protezione contro fonti di rischio non umane

La sede dell'ente risulta in regola con le norme sulla sicurezza dei luoghi di lavoro.

Valutazione : Accettabile

Politica di tutela della privacy

E' stato incaricato il Responsabile della protezione dei dati.

Valutazione : Accettabile

Gestione dei rischi

Sono redatti i registri dei trattamenti dei dati, la valutazione dei processi e dell'impatto della protezione dei dati.

Valutazione : Accettabile

Gestione del personale

I dipendenti vengono regolarmente formati e una volta che cessa il rapporto di lavoro vengono ritirati l'identificativo di accesso e l'account.

Valutazione : Accettabile

Gestione dei terzi che accedono ai dati

I collaboratori e i partner esterni sono sottoposti alle stese regole e procedure per la tutela dei dati dei dipendenti.

Valutazione : Accettabile

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatto trascurabile o limitato.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Perdita di dati o uso improprio dei dati.

Quali sono le fonti di rischio?

Fonti di rischio interne, esterne o non umane

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Minimizzazione dei dati, Lotta contro il malware, Backup, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestione del personale, Gestione dei terzi che accedono ai dati

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, Il rischio è trascurabile o limitato.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Il rischio è trascurabile o limitato.

Valutazione : Accettabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatto limitato o significativo.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Errore materiale, evento doloso o abuso di ufficio da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati.

Quali sono le fonti di rischio?

Fonti umane interne., Fonti umane esterne., Fonti non umane.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Controllo degli accessi fisici, Minimizzazione dei dati, Lotta contro il malware, Backup, Protezione contro fonti di rischio non umane, Gestione del personale, Gestione dei terzi che accedono ai dati

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Importante, trascurabile o limitato.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Importante, trascurabile o limitato.

Valutazione : Accettabile

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Impatto limitato o significativo.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Errore materiale, evento doloso o abuso di ufficio da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati.

Quali sono le fonti di rischio?

Fonti umane interne ed esterne, fonti non umane.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Vulnerabilità, Lotta contro il malware, Backup, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Protezione contro fonti di rischio non umane, Controllo degli accessi fisici, Gestione dei rischi, Gestione del personale, Gestione dei terzi che accedono ai dati

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, trascurabile o limitato.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Importante, trascurabile o limitato.

Valutazione : Accettabile

Piano d'azione

Panoramica

Principi fondamentali

- Finalità
- Basi legali
- Adeguatezza dei dati
- Esattezza dei dati
- Periodo di conservazione
- Informativa
- Raccolta del consenso
- Informativa
- Diritto di rettifica e diritto di cancellazione
- Diritto di limitazione e diritto di opposizione
- Responsabili del trattamento
- Trasferimenti di dati

Misure esistenti o pianificate

- Anonimizzazione
- Controllo degli accessi logici
- Tracciabilità
- Archiviazione
- Sicurezza dei documenti cartacei
- Minimizzazione dei dati
- Vulnerabilità
- Lotta contro il malware
- Backup
- Manutenzione
- Sicurezza dei canali informatici
- Controllo degli accessi fisici
- Sicurezza dell'hardware
- Protezione contro fonti di rischio non umane
- Politica di tutela della privacy
- Gestione dei rischi
- Gestione del personale
- Gestione dei terzi che accedono ai dati

Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati

Misure Migliorabili
Misure Accettabili

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

Panoramica dei rischi

Impatti potenziali

- Impatto trascurabile o limi...
- Impatto limitato o signific...

Minaccia

- Perdita di dati o uso impro...
- Errore materiale, evento do...

Fonti

- Fonti di rischio interne, e...
- Fonti umane interne.
- Fonti umane esterne.
- Fonti non umane.
- Fonti umane interne ed este...

Misure

- Controllo degli accessi log...
- Tracciabilità
- Archiviazione
- Sicurezza dei documenti car...
- Minimizzazione dei dati
- Lotta contro il malware
- Backup
- Sicurezza dei canali inform...
- Controllo degli accessi fis...
- Sicurezza dell'hardware
- Gestione del personale
- Gestione dei terzi che acce...
- Protezione contro fonti di ...
- Vulnerabilità
- Manutenzione
- Gestione dei rischi

Accesso illegittimo ai dati

Gravità : Limitata

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Importante

Probabilità : Importante

Perdita di dati

Gravità : Importante

Probabilità : Importante

Mappaggio dei rischi

- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

11/06/2018