

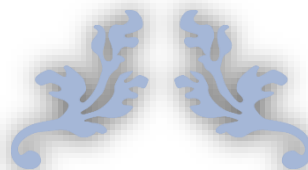


*Comune di  
Monte di Procida*



MODELLO  
ORGANIZZATIVO  
PRIVACY

COMUNE DI MONTE DI PROCIDA



*Via Panoramica - 80070 Monte di Procida (NA)*

*Tel. 081.8684201 - C.F.: 80100130634*

*Pec: [protocollo@pec.comune.montediprocida.na.it](mailto:protocollo@pec.comune.montediprocida.na.it)*



## INTRODUZIONE

Scopo del presente (*Registro Unico delle attività di trattamento dei dati del Comune di Monte di Procida, di seguito denominato semplicemente "Titolare"*), redatto ai sensi della vigente normativa in materia di tutela della Privacy, è la ricognizione dei trattamenti e delle loro principali caratteristiche (finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione) effettuati dall'Amministrazione nello svolgimento dei propri compiti.

In particolare:

1. Ogni Titolare del trattamento e, ove applicabile, il suo Rappresentante tengono un Registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
  - a) Il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del trattamento, del Rappresentante del Titolare del trattamento e del Responsabile della protezione dei dati;
  - b) Le finalità del trattamento;
  - c) Una descrizione delle categorie di interessati e delle categorie di dati personali;
  - d) Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
  - e) Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
  - f) Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  - g) Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32.
2. Ogni Responsabile del trattamento e, ove applicabile, il suo Rappresentante tengono un Registro di tutte le categorie di attività relative al trattamento svolte per conto di un Titolare del trattamento, contenente:



# COMUNE DI MONTE DI PROCIDA

*Provincia di Napoli*



GARANTEPRIVACYITALIA.it

- a) Il nome e i dati di contatto del Responsabile o dei Responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il responsabile del trattamento, del Rappresentante del Titolare del trattamento o del Responsabile del trattamento e, ove applicabile, del Responsabile della protezione dei dati;
  - b) Le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
  - c) Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
  - d) Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32.
3. I Registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
4. Su richiesta, il Titolare del trattamento o il Responsabile del trattamento e, ove applicabile, il Rappresentante del Titolare del trattamento o del Responsabile del trattamento mettono il Registro a disposizione dell'Autorità di controllo.
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10."



## RIFERIMENTI NORMATIVI

- Codice in materia di dati personali (D.Lgs. n.196/2003);
- Linee guida e raccomandazioni del Garante;
- GDPR UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016;
- Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;
- D.Lgs. n. 51/2018;
- D.Lgs. n. 101/2018 di adeguamento ed armonizzazione della normativa interna al GDPR;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- 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;
- 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 GDPR - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e de nozione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- 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;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali ("Data Breach") - WP250 adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Norme internazionali;
- Regolamenti comunali interni, approvati dal Titolare (Consiglio comunale);



## DEFINIZIONI

Il presente documento recepisce e utilizza le seguenti definizioni:

- "GDPR": 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 (GDPR generale sulla protezione dei dati);
- "WP29": gruppo di lavoro articolo 29 sulla protezione dei dati, per tale dovendosi intendere il Gruppo di lavoro istituito in virtù dell'articolo 29 della direttiva 95/46/CE quale organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata con i suoi compiti fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE;
- "Regolamenti comunali interni": il Regolamento interno, approvato dal Titolare del trattamento;
- "ID": identificativo

Recepisce e utilizza, altresì, le seguenti definizioni:

*A) ai fini del D.Lgs. n. 196/2003 e s.m.i (D.Lgs. n. 101/2018):*

- "Trattamento": qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- "Dato personale": qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "Dati identificativi": i dati personali che permettono l'identificazione diretta dell'interessato;



# COMUNE DI MONTE DI PROCIDA

*Provincia di Napoli*



GARANTEPRIVACYITALIA.it

- "Dati sensibili" i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- "Dati giudiziari": i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- "Titolare": la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro Ente, associazione od organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- "Responsabile": la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro Ente, associazione od organismo preposti dal Titolare al trattamento di dati personali;
- "Incaricati": le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- "Interessato": la persona fisica, cui si riferiscono i dati personali;
- "comunicazione": il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal Rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "Diffusione": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "Dato anonimo": il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- "Blocco": la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- "Banca di dati": qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- "Garante": l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675,



- "Comunicazione elettronica": ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;
- "Chiamata": la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;
- "Reti di comunicazione elettronica": i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- "Rete pubblica di comunicazioni": una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;
- "Servizio di comunicazione elettronica": i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
- "Contraente": qualunque persona fisica, persona giuridica, Ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
- "Utente": qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;



# COMUNE DI MONTE DI PROCIDA

*Provincia di Napoli*



GARANTEPRIVACYITALIA.it

- "Dati relativi al traffico": qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- "Dati relativi all'ubicazione": ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
- "Strumenti elettronici": gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- "Autenticazione informatica": l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- "Credenziali di autenticazione": i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- "Parola chiave": componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- "Profilo di autorizzazione": l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- "Sistema di autorizzazione": l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
- "Violazione di dati personali": violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico;
- "Scopi storici": le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- "Scopi statistici": le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;



- "Scopi scientifici": le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore;

## *B) ai fini del "GDPR":*

- «Dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- «Trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- «Limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- «Profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- «Pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- «Archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;



- «Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- «Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- «Destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- «Terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il Responsabile del trattamento e le Persone Autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
- «Consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- «Violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- «Dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;



- «Dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- «Dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- «Stabilimento principale»:
  - a) per quanto riguarda un Titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua Amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
  - b) con riferimento a un Responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua Amministrazione centrale nell'Unione o, se il Responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del Responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del Responsabile del trattamento nella misura in cui tale Responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
- «Rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del Regolamento;
- «Impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- «Gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- «Norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un Titolare del trattamento o Responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di



trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

- «Autorità di controllo»: l'Autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
- «Autorità di controllo interessata»: un'Autorità di controllo interessata dal trattamento di dati personali in quanto:
  - a) Il Titolare del trattamento o il Responsabile del trattamento è stabilito sul territorio dello Stato membro di tale Autorità di controllo;
  - b) Gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
  - c) Un reclamo è stato proposto a tale autorità di controllo;
- «Trattamento transfrontaliero»:
  - a) Trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
  - b) Trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare del trattamento o Responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- «Obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del Regolamento, oppure che l'azione prevista in relazione al Titolare del trattamento o Responsabile del trattamento sia conforme al Regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
- «Servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
- «Organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.



# **REGISTRO UNICO DELLE ATTIVITÀ DI TRATTAMENTO**

Art. 30 comma 1 Regolamento U.E. 679/2016

\* Vedi allegato



## CAMPO DI APPLICAZIONE

Il presente documento si riferisce a tutti i dati trattati direttamente dal Titolare o, per incarico dello stesso, gestiti all'esterno presso terzi, sia con strumenti elettronici o comunque automatizzati che con altri strumenti e supporti, anche non elettronici, e si applica alle sedi sotto identificate:

DENOMINAZIONE SEDE	INDIRIZZO
Sede Municipale (Centrale)	Via Panoramica - 80070 Monte di Procida (NA) - <i>ITALY</i>
Sede Decentrata	
Sede Decentrata	



# COMUNE DI MONTE DI PROCIDA

Provincia di Napoli



GARANTEPRIVACYITALIA.it

## ORGANIGRAMMA PRIVACY

- ❖ Il **“Titolare del trattamento”**: è la “figura” di vertice cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza dei dati.

COMUNE DI MONTE DI PROCIDA			
Indirizzo	CAP/Provincia/Stato	Telefono/Fax	Contatti
Via Panoramica	80070 Monte di Procida (NA) - Italy	Tel. 081.8684201	PEC: <a href="mailto:protocollo@pec.comune.montediprocida.na.it">protocollo@pec.comune.montediprocida.na.it</a>
SINDACO/LEGALE RAPPRESENTANTE			
Nome/Cognome	Data di nascita	Data elezione/nomina	Contatti
Dott. Giuseppe Pugliese	16/03/1978	___/___/20___	E-mail: <a href="mailto:sindaco@comune.montediprocida.na.it">sindaco@comune.montediprocida.na.it</a>

1. Il **“Responsabile/Designato (interno) del trattamento”**: è un soggetto designato dal Titolare che, per esperienza, capacità ed affidabilità, fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza. Nell’ambito del Comune il Responsabile/Designato del trattamento è generalmente individuabile nelle figure apicali, salvo limitate eccezioni. Lo si definisce anche Responsabile “interno” per distinguerlo dal Responsabile “esterno”. Relativamente ai trattamenti di dati personali trasversali a più strutture, per l’individuazione si applica il criterio del maggiore ambito decisionale attribuito o vi possono essere situazioni di co-responsabilità.



# COMUNE DI MONTE DI PROCIDA

Provincia di Napoli



GARANTEPRIVACYITALIA.it

## SEGRETARIO COMUNALE

**Dott.ssa Laura Simioli**

Tel/Fax: 081.8684226

PEC/Mail: [segretario@comune.montediprocida.na.it](mailto:segretario@comune.montediprocida.na.it)

**RUOLO E FUNZIONI** - (Art. 97 del D. Lgs. N. 267/2000 "Testo Unico delle Leggi sull'ordinamento degli Enti Locali")

IL SEGRETARIO COMUNALE SVOLGE COMPITI DI COLLABORAZIONE E FUNZIONI DI ASSISTENZA GIURIDICO – AMMINISTRATIVA NEI CONFRONTI DEGLI ORGANI DELL'ENTE IN ORDINE ALLA CONFORMITÀ DELL'AZIONE AMMINISTRATIVA ALLE LEGGI, ALLO STATUTO ED AI REGOLAMENTI; SOVRINTENDE ALLO SVOLGIMENTO DELLE FUNZIONI DEI DIRIGENTI E NE COORDINA L'ATTIVITÀ (*salvo quando, ai sensi e per gli effetti del Comma 1 dell'articolo 108, il Sindaco abbia nominato il Direttore Generale*).

## SETTORE UOR 1

Capo settore: **Dott.ssa Giovanna Romeo**

Tel/Fax: 081.8684216/ 081.8682579

PEC/Mail: [segreteria@comune.montediprocida.na.it](mailto:segreteria@comune.montediprocida.na.it)

AFFARI GENERALI

SEGRETERIA

STAFF

PROTOCOLLO

SPORT



# COMUNE DI MONTE DI PROCIDA

Provincia di Napoli



GARANTEPRIVACYITALIA.it

## SETTORE UOR 13

Capo settore: *Arch. Antonio Illiano*

Tel/Fax: 081.8684239

PEC/Mail: [demanio@comune.montediprocida.na.it](mailto:demanio@comune.montediprocida.na.it)

GARE

PATRIMONIO

DEMANIO

ANTICORRUZIONE

## SETTORE UOR 3

Capo settore: *Ing. Salvatore Rossi*

Tel/Fax: 081.8684232

PEC/Mail: [ediliziaprivata@comune.montediprocida.na.it](mailto:ediliziaprivata@comune.montediprocida.na.it) / [protezionecivile@comune.montediprocida.na.it](mailto:protezionecivile@comune.montediprocida.na.it)

LAVORI PUBBLICI

URBANISTICA

EDILIZIA

PUBBLICA ILLUMINAZIONE

ACQUEDOTTO

FOGNE



# COMUNE DI MONTE DI PROCIDA

Provincia di Napoli



GARANTEPRIVACYITALIA.it

## SETTORE UOR 4 - UOR 11

Capo settore: **Mario Scamardella**

Tel/Fax: 081.8684241

PEC/Mail: [tributi@comune.montediprocida.na.it](mailto:tributi@comune.montediprocida.na.it) / [mario.scamardella@comune.montediprocida.na.it](mailto:mario.scamardella@comune.montediprocida.na.it)

TRIBUTI

PUBBLICITÀ E AFFISSIONI

COMMERCIO ED ATTIVITÀ PRODUTTIVE

CED ED INNOVAZIONE TECNOLOGICA

## SETTORE UOR 5

Capo settore: **Dott.ssa Michela Di Colandrea**

Tel/Fax: 081.8684212

PEC/Mail: [ragioneria@comune.montediprocida.na.it](mailto:ragioneria@comune.montediprocida.na.it)

RAGIONERIA

BILANCIO



# COMUNE DI MONTE DI PROCIDA

Provincia di Napoli



GARANTEPRIVACYITALIA.it

## SETTORE UOR 7

Capo settore: ***Dott.ssa Concetta Scuotto***

Tel/Fax: 081.8684245

PEC/Mail: [anagrafe@comune.montediprocida.na.it](mailto:anagrafe@comune.montediprocida.na.it) / [personale@comune.montediprocida.na.it](mailto:personale@comune.montediprocida.na.it)

ANAGRAFE

STATO CIVILE

ELETTORALE

ECONOMATO

PERSONALE

## SETTORE UOR 12

Capo settore: ***Capuano Antonio***

Tel/Fax: 081.8684246

PEC/Mail: [servizisociali@comune.montediprocida.na.it](mailto:servizisociali@comune.montediprocida.na.it)

ASSISTENZA

TURISMO E CULTURA

CIMITERO



# COMUNE DI MONTE DI PROCIDA

Provincia di Napoli



GARANTEPRIVACYITALIA.it

## SETTORE UOR 8

Capo settore: **Avv. *Ciro Pugliese***

Tel/Fax: 081.8684223

PEC/Mail: [ciro.pugliese@comune.montediprocida.na.it](mailto:ciro.pugliese@comune.montediprocida.na.it)

AVVOCATURA

CONTENZIOSO

DATORE DI LAVORO

TUTELA DATI PERSONALI

## SETTORE UOR 9

Capo settore: **Dott. *Ugo Mancino***

Tel/Fax: 081.8684247/081.8684234

081 8684254 - Ufficio Contravvenzioni

081 8681609 - Vigili Urbani

PEC/Mail: [polizialocale@comune.montediprocida.na.it](mailto:polizialocale@comune.montediprocida.na.it)/[ufficiocontravvenzioni@comune.montediprocida.na.it](mailto:ufficiocontravvenzioni@comune.montediprocida.na.it)

POLIZIA MUNICIPALE

VIABILITÀ PARCHEGGI

TRASPORTI

RANDAGISMO



# COMUNE DI MONTE DI PROCIDA

*Provincia di Napoli*



GARANTEPRIVACYITALIA.it

## SETTORE UOR 10

Capo settore: ***Dott.ssa Giovanna Romeo***

Tel/Fax: 081.8684216

PEC/Mail: [igieneurbana@comune.montediprocida.na.it](mailto:igieneurbana@comune.montediprocida.na.it) / [istruzione@comune.montediprocida.na.it](mailto:istruzione@comune.montediprocida.na.it)

IGIENE URBANA

SALUTE - PUBBLICA ISTRUZIONE



# COMUNE DI MONTE DI PROCIDA

Provincia di Napoli



GARANTEPRIVACYITALIA.it

2. Il **“Responsabile esterno del trattamento”**: è la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, associazione od organismo, esterno all’Amministrazione, che, previa designazione formale del Titolare (o da un Suo Designato “interno”), assume poteri decisionali su un determinato trattamento e deve attenersi, nelle operazioni svolte, alle istruzioni ricevute. *\*In fase di aggiornamento*

SOGGETTO	ATTIVITA'	DURATA
2I PROJECT SRL Piazza della Barcaiola, 22 80056 Ercolano (NA) P. IVA 06812811211 - Ing. Ivan Iacomino nato a Napoli (NA) il 19/1/1988 Codice Fiscale CMNVNI88A19F839C residente in via Della Barcaiola, 22 80056 Ercolano (NA) <b>è il RSPP.</b> - Il dott. Sorrentino Raffaele, nato a Napoli 27/7/70 Codice Fiscale SRRRFL70L27F839K residente in Mariglianella (NA) <b>è il Medico Competente.</b>	FORNITURA DEI SERVIZI DI GESTIONE INTEGRATA DELLA SALUTE E SICUREZZA SUI LUOGHI DI LAVORO (RSPP – MEDICO COMPETENTE)	DAL __/__/__ AL __/__/__ <i>*In fase di aggiornamento</i>
HALLEY CAMPANIA SRL Via Nazionale N. 135 83013 Mercogliano (AV) - P.IVA 01583190648	AFFIDAMENTO ELABORAZIONE CEDOLINI E CONNESSI ADEMPIMENTI FISCALI E TELEMATICI FORNITORE E SOFTWARE HOUSE CONTABILITÀ FINANZIARIA	DAL __/__/__ AL __/__/__ <i>*In fase di aggiornamento</i>
XXXXXXXXXX SRL VIA XXXXXXXXXXXXXXX N. XX XXXXXXXXXXXXXXXXXXXXXXXXXXXXX <i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>



3. **L'Amministratore di Sistema:** è, in ambito informatico, la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali; *\*In fase di valutazione condizioni di nomina*

Denominazione	Servizio svolto	Estremi Atto di nomina	Durata affidamento

4. **Custode delle credenziali di autenticazione:** il soggetto preposto alla custodia delle password (o che abbia accesso ad informazioni che riguardano le stesse) ed a predisporre nuove password da attribuire ad eventuali nuovi incaricati e revocare quelle non utilizzate per un periodo superiore a sei mesi; *\*In fase di nomina*

Denominazione	Settore	Estremi Atto di nomina



5. **L'incaricato (persona Autorizzata al trattamento):** è la persona fisica che, operando sotto l'autorità del Titolare o del Responsabile, effettua le operazioni di trattamento dei dati, attenendosi alle istruzioni ricevute.

Con apposita Determina del proprio Dirigente/Responsabile/Capo Settore, la persona autorizzata si impegna ad esercitare l'incarico con l'osservanza delle prescrizioni impartite, ovvero:

- ✓ Effettuare sui dati solo le operazioni inerenti alle proprie funzioni e trattarli in modo lecito e secondo correttezza;
- ✓ Verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;
- ✓ Verificare l'esattezza ed il grado di aggiornamento dei dati trattati;
- ✓ Adottare idonee misure tecniche e organizzative, atte a garantire la sicurezza dei trattamenti, oltre quelle indicate e predisposte dal Titolare e dal Responsabile del trattamento
- ✓ Garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli e a non divulgare, neanche dopo la cessazione dell'incarico di Persona Autorizzata, alcuna delle informazioni di cui è venuto a conoscenza nell'adempimento dei compiti assegnatigli, sia perché connesso con tali attività che per caso fortuito (art. 28 par. 3 lettera B del Regolamento UE 2016/679);
- ✓ Utilizzare le informazioni e i dati con cui entra in contatto esclusivamente per lo svolgimento delle attività istituzionali, con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso;
- ✓ Ove applicabile, rispettare l'obbligo di riservatezza in ottemperanza alle norme deontologiche caratteristiche della professione esercitata secondo le norme vigenti (art. 28 par. 3 lettera b Regolamento UE 2016/679)
- ✓ Non cedere ad alcun soggetto, compresi gli interessati, nemmeno in consultazione né in comunicazione né in diffusione i dati conferiti o gestiti per l'effettuazione del servizio.
- ✓ Accedere ai dati utilizzando tutte le disposizioni di sicurezza impartite, quali, a titolo esemplificativo ma non esaustivo, l'uso della ID e PW personali da non cedere ad alcuno, effettuare sui dati solo le operazioni inerenti alla propria mansione, segnalare le anomalie riscontrate.



# COMUNE DI MONTE DI PROCIDA

Provincia di Napoli



GARANTEPRIVACYITALIA.it

- ✓ Conservare correttamente i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che gli stessi siano accessibili a persone non autorizzate;
- ✓ Astenersi dal comunicare a terzi dati e informazioni, senza la preventiva specifica autorizzazione del Titolare o Responsabile del trattamento (salvo i casi previsti dalla legge);
- ✓ Segnalare al Titolare o Responsabile del trattamento, eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- ✓ Informare il Titolare e/o il Responsabile, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali c.d. "Data Breach";

*\*In fase di aggiornamento*

DIPENDENTE	SETTORE	MANSIONE	E MAIL
<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>
<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>
<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>
<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>	<i>*In fase di aggiornamento</i>



6. **Il Responsabile della protezione dei dati - DPO "Data Protection Officer":** è il soggetto che, coadiuva il Titolare ed il Responsabile del trattamento e gli incaricati nella corretta gestione ed applicazione dei principi definiti dal Regolamento Europeo in termini di "Data Protection".

Ha il compito di:

- rendere noti al Titolare o al Responsabile del Trattamento gli obblighi derivanti dal Regolamento Europeo e conservare la documentazione relativa a tale attività di comunicazione o di consulenza;
- vigilare sulla corretta applicazione delle policy in materia di privacy,
- attribuire le responsabilità ad altri soggetti che all'interno dell'Ente operano su dati personali;
- vagliare la corretta attuazione delle disposizioni contenute nel Regolamento Europeo, occupandosi, in particolare di verificare che i sistemi, sin dalla fase della loro progettazione rispettino la privacy ("Privacy by Design") verificare la protezione di default di dati e sistemi ("Privacy by Default"), rilevare che venga garantita la sicurezza nei trattamenti;
- fornire agli interessati un riscontro circa i diritti previsti dal Regolamento;
- garantire la conservazione dei documenti relativi ai trattamenti;
- verificare il tracciamento delle violazioni dei dati personali e la loro comunicazione agli interessati;
- verificare che Titolare o Responsabile effettuino la valutazione dell'impatto delle attività sulla privacy e controllare che venga richiesta l'autorizzazione all'Autorità quando occorre;
- fungere da intermediario tra Titolare o Responsabile e autorità Garante in materia di trattamento dei dati;
- controllare che siano rispettati eventuali provvedimenti o richieste espresse dall'Autorità Garante in materia di trattamento dei dati.
- elaborazione delle procedure inerenti il trattamento dei dati per le varie attività dell'Ente;
- formare ed informare il personale in materia di privacy e trattamento dei dati;



## RPD/DPO

### *Responsabile della protezione dei dati - "Data Protection Officer":*

Determina Affidamento Incarico -	Determina del Responsabile Settore n° 58 del 15.06.2018 – Reg. Gen. N° 573 del 15.06.2018
Atto di nomina DPO	Decreto Sindacale Prot. n. 9850 del 28/6/2018
Ragione sociale	Multibusiness Srl – “GarantePrivacyItalia”
Legale Rappresentante	Dott. Fabrizio D’agostino
DPO/Referente del Team individuato	Dott. Pasquale Nicolazzo
Indirizzo Sede Legale-Operativa	Via dei Bizantini, 37/B 88046 – Via Cristoforo Colombo, 40 88046 Lamezia Terme (CZ)
Cod.Fiscale/P. Iva	03051550790
Telefono/Fax	0968.462702 – 0968.464273
PEC/E-mail	<a href="mailto:dpo@pec.garanteprivacyitalia.it">dpo@pec.garanteprivacyitalia.it</a> - <a href="mailto:info@garanteprivacyitalia.it">info@garanteprivacyitalia.it</a>
Periodo incarico (inizio/fine)	28.06.2018 – 27.06.2019



**Sanzioni:** il presente documento pone quindi una serie di istruzioni, direttive e linee guida poste a salvaguardia dei dati dei soggetti di cui il Comune gestisce i dati, costituenti tutti e ciascuna di essi dati patrimonio dell'Ente stesso. Pertanto, l'eventuale inosservanza o violazione di tali istruzioni, direttive e linee guida costituisce infrazione disciplinare, nonché grave inadempimento ai sensi e per gli effetti dell'art. 1453 del Codice Civile, suscettibile di produrre le conseguenze previste dalla legge, nonché dal contratto collettivo nazionale e individuale di lavoro.

## IL GARANTE DELLA PRIVACY

Il Garante per la protezione dei dati personali è un organo collegiale, composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile. L'attuale Collegio è stato eletto dal Parlamento (ai sensi dell'art. 153, comma 2 del Codice) il 6 giugno 2012 e si è insediato 19 giugno 2012. Attualmente è così composto: Antonello Soro (*Presidente*), Augusta Iannini (*Vice Presidente*), Giovanna Bianchi Clerici, Licia Califano. Il Segretario Generale è il Dott. Giuseppe Busia, coadiuvato da due vice-segretari generali, il Dott. Daniele De Paoli e il Dott. Claudio Filippi. L'Autorità Garante per la protezione dei dati personali è stata istituita al fine di tenere un registro generale dei trattamenti e di controllare se i trattamenti siano effettuati nel rispetto della relativa disciplina, alle dipendenze del Garante è posto uno specifico Ufficio.



## IDENTIFICAZIONE DELLE RISORSE E DELLE INFRASTRUTTURE

Le principali risorse che intervengono nel trattamento dei dati del Titolare sono identificate da:

- Luoghi fisici;
- Sistema informativo.

Di seguito verrà data una descrizione sommaria di questi due elementi.

### *Luoghi Fisici*

I luoghi fisici dove si svolge il trattamento dei dati sono identificati nel Capitolo “Campo di applicazione”.

### *Sistema Informativo e risorse elaborative*

*\*Vedi allegato DPS ed Assessment tecnologico*



## ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

*\*Vedi allegato DPS ed Assessment tecnologico*



## MISURE IN ESSERE E DA ADOTTARE

### Contenuti

In questa sezione vanno riportate, in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

### Informazioni essenziali

In ogni tabella vanno indicate le seguenti informazioni:

- ☐ Struttura di riferimento: Settore/Servizio;
- ☐ Oggetto Banca Dati;
- ☐ Misure: vanno descritte sinteticamente le misure adottate specificando se la misura è già in essere o da adottare, con eventuale indicazione, in tale ultimo caso, dei tempi previsti per la sua messa in opera.
- ☐ Descrizione dei rischi: per ciascuna misura sono indicati sinteticamente i rischi che si intendono contrastare.

SETTORE \_\_\_\_\_

SERVIZIO	OGGETTO BANCA DATI	MISURA GIÀ IN ESSERE	Misura da adottare (tempi previsti per l'adozione delle misure)	DESCRIZIONE DEI RISCHI CONTRASTATI
----------	--------------------------	-------------------------	---	---------------------------------------

*\*In fase di aggiornamento*



## IL SISTEMA DI PROTEZIONE E I DIRITTI DEGLI INTERESSATI

### *Modalità per l'esercizio dei diritti*

Trasparenza e modalità trasparenti per l'esercizio dei diritti dell'interessato sono alla base della disciplina del "GDPR". In particolare, il Titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura tecnica e organizzativa a ciò idonea. Benché sia il solo Titolare a dover dare riscontro in caso di esercizio dei diritti, il Responsabile è tenuto a collaborare con il Titolare o un suo delegato ai fini dell'esercizio di tali diritti. L'esercizio è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni. Il Titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee. Sono ammesse deroghe ai diritti riconosciuti dal "GDPR", ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici. Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso):

- ✓ 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; il Titolare o un suo delegato deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Spetta al Titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12.5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il Titolare o un suo delegato deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.



## *Diritto di accesso*

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 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

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 ai sensi dell'articolo 46 relative al trasferimento.

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. 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.

Il diritto di ottenere una copia di cui al paragrafo 3 dell'art. 15 GDPR non deve ledere i diritti e le libertà altrui.



## *Diritto alla rettifica e cancellazione*

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.

Quanto al diritto cosiddetto "*all'Oblío*", l'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
- c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
- d) i dati personali sono stati trattati illecitamente;
- e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento;
- f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, par. 1.

Il Titolare, se ha reso pubblici dati personali ed è obbligato a cancellarli ai sensi del paragrafo 1, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

I paragrafi 1 e 2 non si applicano 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;
- d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
- e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il Titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

### *Diritto alla limitazione*

L'interessato ha il diritto di ottenere dal Titolare del trattamento 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 del trattamento 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, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del paragrafo 1, 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.

L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal Titolare del trattamento prima che detta limitazione sia revocata. 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. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

### *Diritto alla portabilità*

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del trattamento e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti qualora:

- a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
- b) il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro, se tecnicamente fattibile. L'esercizio del diritto alla portabilità lascia impregiudicato il diritto alla cancellazione. Tale diritto 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.

### *Diritto di opposizione e processo decisionale automatizzato relativo alle persone*

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) GDPR, compresa la profilazione sulla base di tali disposizioni. Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di 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. Il diritto di cui ai paragrafi 1 e 2 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. 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. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 "GDPR", 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.



## VIOLAZIONE O PERDITA DEI DATI – “DATA BREACH”

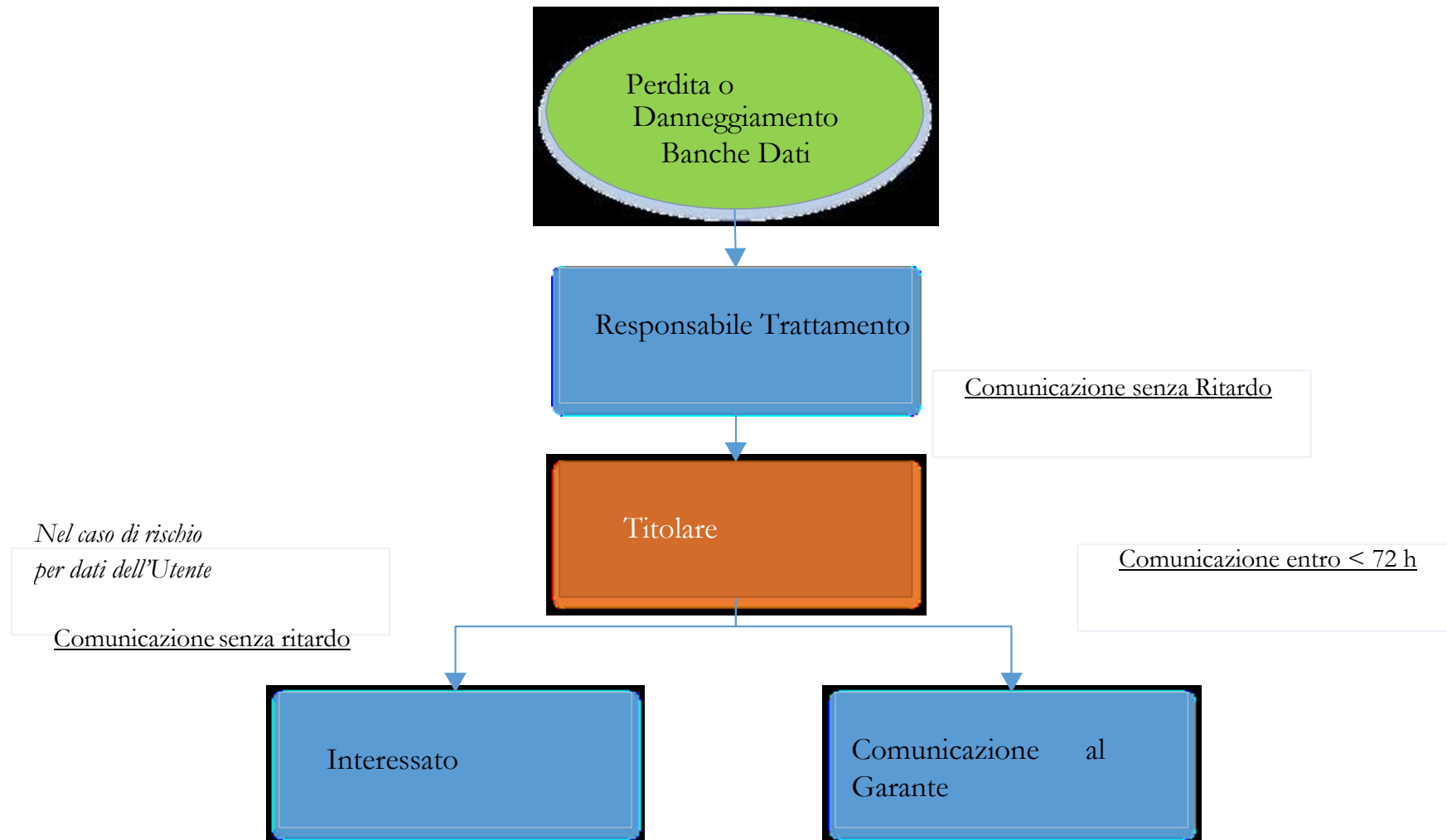
Nel caso in cui ci sia una violazione dei dati personali, intesa come la "violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ad informazioni personali trasmesse, memorizzate o comunque trattate, l'Ente è tenuto a darne comunicazione all'Autorità competente.

Entro 72 ore dalla conoscenza del fatto, le Amministrazioni Pubbliche sono tenute a comunicare al Garante (tramite apposito modello pubblicato sul sito [www.garanteprivacy.it](http://www.garanteprivacy.it)) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali.

La comunicazione deve:

1. Descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2. Identificare il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
3. Descrivere le probabili conseguenze della violazione dei dati personali;
4. Descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Inoltre, quando la violazione dei dati personali è suscettibile di danno per i diritti e le libertà delle persone fisiche, il Titolare deve comunicare la violazione anche all'interessato, senza ingiustificato ritardo, descrivendola con un linguaggio semplice e chiaro (salve circostanze al verificarsi delle quali la comunicazione è esclusa).





## FORMAZIONE

La gestione della sicurezza dei dati in una qualsiasi organizzazione vede coinvolte in modo stretto gli utenti del sistema. Ciò richiede un piano di formazione ed informazione rivolto ai dipendenti e a tutti coloro che utilizzano le risorse (informatiche/cartacee) dell'organizzazione. L'obiettivo è quello di creare la "cultura della sicurezza" attraverso una serie di attività volte ad illustrare i provvedimenti ed i comportamenti da adottare per migliorare la sicurezza nel trattamento dei dati. Il piano è stato studiato, organizzato e suddiviso sulla base delle specifiche esigenze di ciascun Settore in relazione alla natura dei dati trattati e dei rischi generici o specifici che incombono sui dati, nonché dei criteri e delle modalità di evitare tali rischi.

Periodicamente il Responsabile della protezione dei dati del Comune trasmette a tutti i dipendenti del materiale informativo in cui sono riportate le principali regole di gestione ed utilizzo delle risorse del sistema informativo.

### *Piano di formazione e informazione*

Per le risorse umane, che hanno un ruolo chiave nel trattamento di dati personali, verrà inviato e trasmesso del materiale informativo, inerente i principi fondamentali della normativa vigente (D. Lgs. 196/2003 e successive modificazioni ed armonizzazioni - D. Lgs. 101/2018) e in particolar modo del Reg. EU 679/2016. I contenuti essenziali del piano di formazione e informazione sono:

- Ragioni della nuova normativa;
- Ambito di applicazione materiale e territoriale;
- Principi generali;
- Diritti dell'interessato;
- Titolare e responsabili del trattamento;
- "Data Protection Officer";
- Obbligo di tenuta di un "**Registro delle attività di trattamento**" ed effettuazione della "**Valutazione di impatto sulla protezione dei dati**" ove se ne riscontri la necessità;
- Obblighi di consultazione con l'Autorità di controllo;



- Eventuali Codici di condotta e certificazione;
- Trasferimento dei dati e problematiche di diritto extracomunitario;
- Principi legislativi e comunitari;
- Funzionamento della normativa nell'ambito dei diritti del cittadino;
- Crimini informatici, frodi, abusi, danni, casistica;
- Rischi possibili e probabili cui sono sottoposti i dati;
- Misure di sicurezza tecniche ed organizzative e comportamentali deputate alla prevenzione dei rischi;
- Comportamenti e modalità di lavoro per prevenire i rischi;

Tale materiale informativo viene trasmesso mediante supporti informativi cartacei, elettronici e/o telematici.

Il piano di informazione e il materiale informativo verrà trasmesso anche per ai dipendenti neo assunti che nell'ambito delle loro mansioni nel trattamento dei dati, e a tutti coloro che tratteranno dati per conto del Titolare.

Inoltre ogni soggetto autorizzato al trattamento dei dati all'interno dell'Ente, svolgerà un corso di formazione ed informazione (in modalità FAD/E-learnig).



## REVISIONE/ AGGIORNAMENTO/MONITORAGGIO COSTANTE

Il presente Documento è definito di per se “dinamico”, ragion per cui sono previsti aggiornamenti specifici ogniqualvolta si verificano significative variazioni delle situazioni relative ai trattamenti di dati, agli strumenti e ai sistemi informatici utilizzati, nonché eventuali affidamenti esterni, nomine o nuove assunzioni, parimenti con cadenza annuale, il Titolare, coadiuvato dal Responsabile della protezione dei dati e dai Responsabili/Designati interni, effettuerà un monitoraggio sull’efficacia delle misure tecniche e organizzative qui previste al fine di garantire la sicurezza dei trattamenti.

L’originale del presente documento (indipendentemente che sia in forma cartacea o informatica), è custodito presso la Sede Centrale Municipale dell’Ente, per essere esibito in caso di controllo delle Autorità competenti e dimostrare di aver adottato tutte le misure previste dalla vigente normativa sulla tutela e la protezione dei dati personali, ed in particolare quanto dettato dal Regolamento Europeo 679/2016 relativo alla protezione dei dati personali, dimostrando il c.d. “*Principio di Accountability*”.

Una copia del presente Documento è custodita presso la Sede del Responsabile della protezione dei dati – “DPO” nominato dal Comune, ovvero la **Multibusiness Srl** “*GarantePrivacyItalia*”, in Via Cristoforo Colombo, n° 40 – 88046 Lamezia Terme (CZ), fin quando il “DPO” ricoprirà tale incarico presso l’Ente Titolare del trattamento.



# REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEL **COMUNE DI MONTE DI PROCIDA**

In ottemperanza a quanto riportato nell'art. 30 del Regolamento UE 679/2016, di seguito sono riportate tutte le informazioni che costituiscono il Registro delle Attività di Trattamento svolte sotto la propria responsabilità da parte del Titolare del Trattamento ovvero il *Comune di Monte di Procida*.

Dati di contatto sono i seguenti:

**TITOLARE DEL TRATTAMENTO:** Comune di Monte di Procida:

**SEDE:** Via Panoramica - 80070 Monte di Procida (NA)

**CODICE FISCALE:** 80100130634

**TEL.:** 081.8684201 - **FAX:** 081.8682579

**E-MAIL:** [info@comune.montediprocida.na.it](mailto:info@comune.montediprocida.na.it)

**PEC:** [protocollo@pec.comune.montediprocida.na.it](mailto:protocollo@pec.comune.montediprocida.na.it)

## INTRODUZIONE

Il Registro dei trattamenti è un documento che censisce le caratteristiche principali dell'attività del Titolare del trattamento. La sua funzione è prevalentemente descrittiva e il suo contenuto deve corrispondere alla realtà dei fatti. Esso costituisce la base per eseguire gli ulteriori adempimenti (informative, nomine soggetti autorizzati, ecc.).

I soggetti tenuti alla redazione del Registro dei Trattamenti sono individuati dall'art. 30 Reg UE 679/2016.

Il Garante sottolinea inoltre che, a prescindere dall'obbligo normativo, è essenziale predisporre la ricognizione dei trattamenti svolti e delle loro principali caratteristiche (finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il Titolare ritenga opportuna al fine di documentare le attività di trattamento svolte) funzionale all'istituzione del Registro stesso.



## **PERSONALE - GESTIONE DEL RAPPORTO DI LAVORO**

### DESCRIZIONE DEL TRATTAMENTO:

Il trattamento ha per oggetto la gestione del personale dipendente, intesa come la gestione del rapporto di lavoro avviato a qualunque titolo (compreso quelli a tempo determinato, part-time e di consulenza) nell'Ente ovvero in aziende o istituzioni collegate o vigilate, compresi tutti i procedimenti concorsuali o le altre procedure di selezione previste così come per i corsi di formazione. I dati sono oggetto di trattamento presso i diversi Settori/Uffici funzionali e strutture del Comune relativamente alla prestazione del servizio, orario, assenze per malattia o altro e in generale ricezione, registrazione, trasmissione, conservazione, corrispondenza, archiviazione delle delibere di Consiglio e/o di Giunta. Sono compresi nel trattamento tutte le elaborazioni a fini statistici e per le attività di controllo della gestione. Dati afferenti a particolari categorie, quali quelli relativi alle convinzioni religiose filosofiche, sulla vita sessuale o di altro genere possono eventualmente essere compresi tra quelli trattati in caso di accesso a diversi servizi erogati dalla P.A., come quelli sanitari relativi ai familiari dei dipendenti ai fini della concessione di benefici nei casi previsti dalla legge. Tutti i dati pervengono all'Amministrazione su iniziativa dei dipendenti e/o a richiesta e vengono trattati per l'applicazione dei diversi istituti contrattuali disciplinati dalla legge (gestione giuridica, economica, previdenziale, pensionistica, attività di aggiornamento e formazione). È possibile infine l'esecuzione di interrogazioni e incroci con altre banche dati a cui l'Amministrazione ha accesso, per raffronti con amministrazioni e gestori di pubblici servizi, finalizzate all'accertamento d'ufficio di uno stato, qualità o fatto ovvero al controllo a campione o massivo delle dichiarazioni sostitutive rese ai sensi dell'art. 43 del D.P.R. n. 445/2000.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:



FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Gestione del personale	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Origini razziali; Origini etniche; Convinzioni religiose; adesione ad organizzazioni a carattere religioso; Convinzioni filosofiche o di altro genere; adesione ad organizzazioni a carattere filosofico; Adesione a sindacati o organizzazioni a carattere sindacale; Carte sanitarie; Stato di salute - relativo a familiari; Vita sessuale; Dati relativi a condanne penali e reati; Dati relativi alla famiglia o a situazioni personali; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Istruzione e cultura; Beni, proprietà, possesso; Idoneità al lavoro; Coordinate bancarie; Sesso m/f	Norma Unione Europea (GDPR 2016/679)
Gestione delle presenze del personale	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Carte sanitarie; Dati relativi alla famiglia o a situazioni personali; Stato di salute - relativo a familiari	Norma Unione Europea (GDPR 2016/679)
Gestione ferie e malattie	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Stato di salute - relativo a familiari; Dati relativi alla famiglia o a situazioni personali	Norma Unione Europea (GDPR 2016/679)



Gestione permessi	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Convinzioni religiose; adesione ad organizzazioni a carattere religioso; Convinzioni filosofiche o di altro genere; adesione ad organizzazioni a carattere filosofico; Adesione a sindacati o organizzazioni a carattere sindacale; Stato di salute - relativo a familiari; Dati relativi alla famiglia o a situazioni personali	Norma Unione Europea (GDPR 2016/679)
Adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Adesione a sindacati o organizzazioni a carattere sindacale	Norma Unione Europea (GDPR 2016/679)
Adempimenti in materia di assicurazione contro gli infortuni	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Carte sanitarie; Idoneità al lavoro	Norma Unione Europea (GDPR 2016/679)
Adempimenti previdenziali	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Carte sanitarie; Dati relativi alla famiglia o a situazioni personali; Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Norma Unione Europea (GDPR 2016/679)



Adempimenti fiscali	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Convinzioni religiose; adesione ad organizzazioni a carattere religioso; Convinzioni filosofiche o di altro genere; adesione ad organizzazioni a carattere filosofico; Adesione a sindacati o organizzazioni a carattere sindacale; Stato di salute - relativo a familiari; Dati relativi alla famiglia o a situazioni personali; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Beni, proprietà, possesso; Sesso m/f	Norma Unione Europea (GDPR 2016/679)
Trattamento giuridico ed economico del personale	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Origini razziali; Origini etniche; Convinzioni religiose; adesione ad organizzazioni a carattere religioso; Convinzioni filosofiche o di altro genere; adesione ad organizzazioni a carattere filosofico; Adesione a sindacati o organizzazioni a carattere sindacale; Carte sanitarie; Stato di salute - relativo a familiari; Vita sessuale; Dati relativi a condanne penali e reati; Dati relativi alla famiglia o a situazioni personali; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Istruzione e cultura; Beni, proprietà, possesso; Idoneità al lavoro; Coordinate bancarie; Sesso m/f	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:



INTERESSATI
Personale dipendente
Stagisti
Personale pubblico dirigenziale

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili
Convinzioni religiose; adesione ad organizzazioni a carattere religioso	Dati sensibili
Convinzioni filosofiche o di altro genere; adesione ad organizzazioni a carattere filosofico	Dati sensibili
Adesione a sindacati o organizzazioni a carattere sindacale	Dati sensibili
Carte sanitarie	Dati relativi alla salute
Stato di salute - relativo a familiari	Dati relativi alla salute
Vita sessuale	Dati sensibili
Dati relativi a condanne penali e reati	Dati giudiziari
Dati relativi alla famiglia o a situazioni personali	Dati comuni
Lavoro (occupazione, curriculum, ecc.)	Dati comuni
Istruzione e cultura	Dati comuni
Beni, proprietà, possesso	Dati comuni
Idoneità al lavoro	Dati relativi alla salute
Coordinate bancarie	Dati comuni
Sesso m/f	Dati comuni

#### CATEGORIE DI DESTINATARI:

Consulenti e liberi professionisti in forma singola o associata, Enti previdenziali ed assistenziali, Organizzazioni sindacali e patronati, Centri di formazione professionale, Altre amministrazioni pubbliche, Società di Esazione

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita.

## SERVIZI DEMOGRAFICI / ANAGRAFE

### DESCRIZIONE DEL TRATTAMENTO:

Servizi demografici / Anagrafe - Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi demografici / Anagrafe - Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini (residenti e non)

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili
Dati relativi alla famiglia o a situazioni personali	Dati comuni
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Provincia di residenza	Dati comuni
Professione dichiarata	Dati comuni
Sesso m/f	Dati comuni

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita

## SERVIZI DEMOGRAFICI / STATO CIVILE

### DESCRIZIONE DEL TRATTAMENTO:

Servizi demografici / Stato civile - Attività di gestione dei registri di stato civile

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi demografici / Stato civile - Attività di gestione dei registri di stato civile	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili
Dati relativi alla famiglia o a situazioni personali	Dati comuni
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Provincia di residenza	Dati comuni
Professione dichiarata	Dati comuni
Sesso m/f	Dati comuni

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita

## SERVIZI DEMOGRAFICI / ELETTORALE

### DESCRIZIONE DEL TRATTAMENTO:

Servizi demografici / Elettorale - Attività relativa all'elettorato attivo e passivo

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi demografici / Elettorale - Attività relativa all'elettorato attivo e passivo	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili
Dati relativi alla famiglia o a situazioni personali	Dati comuni
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Provincia di residenza	Dati comuni
Professione dichiarata	Dati comuni
Sesso m/f	Dati comuni

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita

## SERVIZI DEMOGRAFICI / ELETTORALE ALBI DEGLI SCRUTATORI

### DESCRIZIONE DEL TRATTAMENTO:

Servizi demografici / Elettorale - Attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi demografici / Elettorale - Attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili
Dati relativi alla famiglia o a situazioni personali	Dati comuni
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Provincia di residenza	Dati comuni
Professione dichiarata	Dati comuni
Sesso m/f	Dati comuni

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita

## SERVIZI DEMOGRAFICI / ELETTORALE DELL'ELENCO DEI GIUDICI POPOLARI

### DESCRIZIONE DEL TRATTAMENTO:

Servizi demografici / Elettorale - Attività relativa alla tenuta dell'elenco dei giudici popolari

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi demografici / Elettorale - Attività relativa alla tenuta dell'elenco dei giudici popolari	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili
Dati relativi alla famiglia o a situazioni personali	Dati comuni
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Provincia di residenza	Dati comuni
Professione dichiarata	Dati comuni
Sesso m/f	Dati comuni

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## SERVIZI DEMOGRAFICI / LEVA OBIETTORI DI COSCIENZA

### DESCRIZIONE DEL TRATTAMENTO:

Servizi demografici / Leva - Attività relativa alla tenuta del registro degli obiettori di coscienza

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi demografici / Leva - Attività relativa alla tenuta del registro degli obiettori di coscienza	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili
Dati relativi alla famiglia o a situazioni personali	Dati comuni
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Provincia di residenza	Dati comuni
Professione dichiarata	Dati comuni
Sesso m/f	Dati comuni

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita

## SERVIZI DEMOGRAFICI / LEVA

### DESCRIZIONE DEL TRATTAMENTO:

Servizi demografici / Leva - Attività relativa alla tenuta delle liste di leva e dei registri matricolari

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi demografici / Leva - Attività relativa alla tenuta delle liste di leva e dei registri matricolari	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili
Dati relativi alla famiglia o a situazioni personali	Dati comuni
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Provincia di residenza	Dati comuni
Professione dichiarata	Dati comuni
Sesso m/f	Dati comuni

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## SERVIZI SOCIALI - ATTIVITÀ RELATIVA ALL'ASSISTENZA DOMICILIARE

### DESCRIZIONE DEL TRATTAMENTO:

Servizi sociali - Attività relativa all'assistenza domiciliare

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi sociali - Attività relativa all'assistenza domiciliare	Dati relativi a condanne penali e reati; Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Origini razziali; Origini etniche; Stato di salute - patologie attuali; Stato di salute - patologie pregresse; Stato di salute - terapie in corso; Stato di salute - relativo a familiari; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Dati relativi al patrimonio immobiliare; Dati relativi alla situazione reddituale	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Soggetti bisognosi di assistenza domiciliare e di aiuti di carattere socio-assistenziale
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Dati relativi a condanne penali e reati	Dati giudiziari
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili
Stato di salute - patologie attuali	Dati relativi alla salute



Stato di salute - patologie pregresse	Dati relativi alla salute
Stato di salute - terapie in corso	Dati relativi alla salute
Stato di salute - relativo a familiari	Dati relativi alla salute
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Dati relativi al patrimonio immobiliare	Dati comuni
Dati relativi alla situazione reddituale	Dati comuni

#### CATEGORIE DI DESTINATARI:

Ente gestore degli alloggi (Comunicazione dei dati all'ente gestore degli alloggi per le procedure di compilazione delle graduatorie e l'assegnazione dei benefici)

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## SERVIZI SOCIALI - ATTIVITÀ RELATIVA A RICOVERO O INSERIMENTO IN ISTITUTI E CASE DI CURA

### DESCRIZIONE DEL TRATTAMENTO:

Servizi sociali - Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi sociali - Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	Dati relativi a condanne penali e reati; Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Origini razziali; Origini etniche; Stato di salute - patologie attuali; Stato di salute - patologie pregresse; Stato di salute - terapie in corso; Stato di salute - relativo a familiari; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Dati relativi al patrimonio immobiliare; Dati relativi alla situazione reddituale	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Soggetti in stato di non autosufficienza psico-fisica
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Dati relativi a condanne penali e reati	Dati giudiziari
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili



Stato di salute - patologie attuali	Dati relativi alla salute
Stato di salute - patologie pregresse	Dati relativi alla salute
Stato di salute - terapie in corso	Dati relativi alla salute
Stato di salute - relativo a familiari	Dati relativi alla salute
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Dati relativi al patrimonio immobiliare	Dati comuni
Dati relativi alla situazione reddituale	Dati comuni

#### CATEGORIE DI DESTINATARI:

Ente gestore degli alloggi (Comunicazione dei dati all'ente gestore degli alloggi per le procedure di compilazione delle graduatorie e l'assegnazione dei benefici)

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## SERVIZI SOCIALI - ATTIVITÀ RICREATIVE

### DESCRIZIONE DEL TRATTAMENTO:

Servizi sociali - Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi sociali - Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale	Dati relativi a condanne penali e reati; Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Origini razziali; Origini etniche; Stato di salute - patologie attuali; Stato di salute - patologie pregresse; Stato di salute - terapie in corso; Stato di salute - relativo a familiari; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Dati relativi al patrimonio immobiliare; Dati relativi alla situazione reddituale	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Dati relativi a condanne penali e reati	Dati giudiziari
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili



Stato di salute - patologie attuali	Dati relativi alla salute
Stato di salute - patologie pregresse	Dati relativi alla salute
Stato di salute - terapie in corso	Dati relativi alla salute
Stato di salute - relativo a familiari	Dati relativi alla salute
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Dati relativi al patrimonio immobiliare	Dati comuni
Dati relativi alla situazione reddituale	Dati comuni

#### CATEGORIE DI DESTINATARI:

Ente gestore degli alloggi (Comunicazione dei dati all'ente gestore degli alloggi per le procedure di compilazione delle graduatorie e l'assegnazione dei benefici)

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## SERVIZI SOCIALI - ATTIVITÀ VALUTAZIONE REQUISITI PER CONCESSIONE DI CONTRIBUTI

### DESCRIZIONE DEL TRATTAMENTO:

Servizi sociali - Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi sociali - Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Dati relativi a condanne penali e reati; Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Origini razziali; Origini etniche; Stato di salute - patologie attuali; Stato di salute - patologie pregresse; Stato di salute - terapie in corso; Stato di salute - relativo a familiari; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Dati relativi al patrimonio immobiliare; Dati relativi alla situazione reddituale	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini
Soggetti che versano in condizioni di indigenza

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Dati relativi a condanne penali e reati	Dati giudiziari
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili



Stato di salute - patologie attuali	Dati relativi alla salute
Stato di salute - patologie pregresse	Dati relativi alla salute
Stato di salute - terapie in corso	Dati relativi alla salute
Stato di salute - relativo a familiari	Dati relativi alla salute
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Dati relativi al patrimonio immobiliare	Dati comuni
Dati relativi alla situazione reddituale	Dati comuni

#### CATEGORIE DI DESTINATARI:

Ente gestore degli alloggi (Comunicazione dei dati all'ente gestore degli alloggi per le procedure di compilazione delle graduatorie e l'assegnazione dei benefici)

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## SERVIZI SOCIALI - ATTIVITÀ DI SOSTEGNO DELLE PERSONE BISOGNOSE DI SERVIZIO PUBBLICO DI TRASPORTO

### DESCRIZIONE DEL TRATTAMENTO:

Servizi sociali - Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Servizi sociali - Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	Dati relativi a condanne penali e reati; Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Origini razziali; Origini etniche; Stato di salute - patologie attuali; Stato di salute - patologie pregresse; Stato di salute - terapie in corso; Stato di salute - relativo a familiari; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Dati relativi al patrimonio immobiliare; Dati relativi alla situazione reddituale	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

Interessati
Soggetti che versano in condizioni di indigenza
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Dati relativi a condanne penali e reati	Dati giudiziari
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili



Stato di salute - patologie attuali	Dati relativi alla salute
Stato di salute - patologie pregresse	Dati relativi alla salute
Stato di salute - terapie in corso	Dati relativi alla salute
Stato di salute - relativo a familiari	Dati relativi alla salute
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Dati relativi al patrimonio immobiliare	Dati comuni
Dati relativi alla situazione reddituale	Dati comuni

#### CATEGORIE DI DESTINATARI:

Ente gestore degli alloggi (Comunicazione dei dati all'ente gestore degli alloggi per le procedure di compilazione delle graduatorie e l'assegnazione dei benefici)

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## ISTRUZIONE E CULTURA - ATTIVITÀ RELATIVA ALLA GESTIONE DEGLI ASILI NIDO, ELEMENTARI E MEDIE

### DESCRIZIONE DEL TRATTAMENTO:

Il trattamento ha per oggetto le attività di gestione delle strutture comunali dei servizi per l'infanzia e degli istituti di istruzione primaria e secondaria inferiore di competenza. Dati degli alunni, relativi a specifiche situazioni patologiche, possono essere comunicati direttamente dalla famiglia e afferiscono a categorie di particolare sensibilità. Ancora, le scelte effettuate per il servizio di mensa (pasti vegetariani o rispondenti a convinzioni religiose) possono rivelare le convinzioni religiose, filosofiche o di altro genere, così come l'origine etnica o razziale è desumibile dalla nazionalità. Tutte o parte delle informazioni raccolte possono essere comunicate a gestori del servizio mensa esterni all'amministrazione pubblica o al soggetti che provvedono all'erogazione del servizio di trasporto scolastico.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Istruzione e cultura - Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	Convinzioni religiose; adesione ad organizzazioni a carattere religioso; Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Origini razziali; Origini etniche; Convinzioni filosofiche o di altro genere; adesione ad organizzazioni a carattere filosofico; Stato di salute - patologie attuali; Stato di salute - patologie pregresse; Stato di salute - terapie in corso; Dati relativi alla situazione reddituale	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Scolari o studenti
Familiari dell'interessato

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
----------------	-----------



Convinzioni religiose; adesione ad organizzazioni a carattere religioso	Dati sensibili
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Origini razziali	Dati sensibili
Origini etniche	Dati sensibili
Convinzioni filosofiche o di altro genere; adesione ad organizzazioni a carattere filosofico	Dati sensibili
Stato di salute - patologie attuali	Dati relativi alla salute
Stato di salute - patologie pregresse	Dati relativi alla salute
Stato di salute - terapie in corso	Dati relativi alla salute
Dati relativi alla situazione reddituale	Dati comuni

#### CATEGORIE DI DESTINATARI:

Gestori esterni delle mense e società di trasporto, Circoscrizioni, Istituti scolastici, Enti convenzionati, Gestori esterni del servizio di trasporto scolastico, Istituti, scuole e università

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## ISTRUZIONE E CULTURA - GESTIONE DELLE BIBLIOTECHE E DEI CENTRI DI DOCUMENTAZIONE

### DESCRIZIONE DEL TRATTAMENTO:

Il trattamento ha per oggetto la gestione delle attività bibliotecarie o dei centri di documentazione le cui collezioni comprendono archivi audiovisivi su qualsiasi supporto, la gestione organizzativa degli addetti all'ingresso, degli assistenti di sala o altre figure professionali e tecniche, la registrazione degli accessi o la prenotazione delle visite nelle sezioni della struttura normalmente chiuse al pubblico. Dati sulle condizioni di salute sono acquisiti per erogare servizi specifici all'utenza, specialmente per superamento di barriere architettoniche ovvero utilizzo di particolari supporti. Ulteriori dati afferenti a categorie sensibili sono desumibili dalle richieste di accesso a collezioni, fondi, singoli volumi, film ovvero a qualsiasi tipo di documento visionato o preso in prestito, nonché da colloqui posti in essere per accertare particolari esigenze di studio dei richiedenti per accedere a sale riservate ad accesso limitato.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Istruzione e cultura - Gestione delle biblioteche e dei centri di documentazione	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Istruzione e cultura; Convinzioni filosofiche o di altro genere; adesione ad organizzazioni a carattere filosofico; Opinioni politiche; Adesione a partiti o organizzazioni a carattere politico; Adesione a sindacati o organizzazioni a carattere sindacale; Stato di salute - patologie attuali	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Clienti o Utenti



I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Istruzione e cultura	Dati comuni
Convinzioni filosofiche o di altro genere; adesione ad organizzazioni a carattere filosofico	Dati sensibili
Opinioni politiche	Dati sensibili
Adesione a partiti o organizzazioni a carattere politico	Dati sensibili
Adesione a sindacati o organizzazioni a carattere sindacale	Dati sensibili
Stato di salute - patologie attuali	Dati relativi alla salute

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## POLIZIA MUNICIPALE - ATTIVITÀ RELATIVA ALL'INFORTUNISTICA STRADALE

### DESCRIZIONE DEL TRATTAMENTO:

Polizia municipale - Attività relativa all'infortunistica stradale

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Polizia municipale - Attività relativa all'infortunistica stradale	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Soggetti coinvolti in incidenti e/o infortuni stradali

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

Personali: Identificativi; Sensibili/Particolari: Salute – Patologie in corso;

### CATEGORIE DI DESTINATARI:

Organi di pubblica sicurezza; Altri: Dipartimento per i trasporti terrestri – Prefettura - Familiari - Assicurazioni;

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## POLIZIA MUNICIPALE - GESTIONE DELLE PROCEDURE SANZIONATORIE

### DESCRIZIONE DEL TRATTAMENTO:

Polizia municipale - Gestione delle procedure sanzionatorie

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Polizia municipale - Gestione delle procedure sanzionatorie	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Soggetti interessati da controlli eseguiti dalle Forze dell'ordine

### CATEGORIA DATI:

Personalì: Identificativi - Abitudini/stile vita/comportamento - Posizione geografica - Immagini/ suoni - Beni/ proprietà/ possessori; Personalì Giudiziari (diversi da condanne penali e reati); Giudiziari: condanne penali e reati;

### CATEGORIE DI DESTINATARI:

Organismi pubblici; Organi di pubblica sicurezza; Fornitori di servizi;

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## POLIZIA MUNICIPALE - ATTIVITÀ DI POLIZIA ANNONARIA, COMMERCIALE ED AMMINISTRATIVA

### DESCRIZIONE DEL TRATTAMENTO:

Polizia municipale - Attività di polizia annonaria, commerciale ed amministrativa

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Polizia municipale - Attività di polizia annonaria, commerciale ed amministrativa	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Soggetti richiedenti licenze o autorizzazioni amministrative

### CATEGORIA DATI:

### CATEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## POLIZIA MUNICIPALE - ATTIVITÀ DI VIGILANZA EDILIZIA, AMBIENTE E SANITÀ, POLIZIA MORTUARIA

### DESCRIZIONE DEL TRATTAMENTO:

Polizia municipale - Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Polizia municipale - Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Soggetti coinvolti in violazioni in materia sanitaria o ambientale
Soggetti deceduti

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

### CATEGORIA DATI:

### CATEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## RILASCIO DELLE LICENZE PER COMMERCIO, PUBBLICO ESERCIZIO, L'ARTIGIANATO E LA PUBBLICA SICUREZZA

### DESCRIZIONE DEL TRATTAMENTO:

Rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Commercianti
Soggetti richiedenti licenze o autorizzazioni amministrative

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

### CATEGORIA DATI:

### CATEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## GESTIONE DEI DATI RELATIVI AGLI ORGANI ISTITUZIONALI DELL'ENTE

### DESCRIZIONE DEL TRATTAMENTO:

Gestione dei dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonché dei rappresentanti dell'ente presso enti, aziende e istituzioni

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Gestione dei dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonché dei rappresentanti dell'ente presso enti, aziende e istituzioni	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Personale dipendente

### CATEGORIA DATI:

### CATEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## ATTIVITÀ POLITICA DI INDIRIZZO E DI CONTROLLO

### DESCRIZIONE DEL TRATTAMENTO:

Attività politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Attività politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Soggetti o organismi pubblici

### CATEGORIA DATI:

### CATEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## PIANIFICAZIONE URBANISTICA

### DESCRIZIONE DEL TRATTAMENTO:

Pianificazione urbanistica, amministrazione del territorio, controlli su illeciti edilizia

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Pianificazione urbanistica, amministrazione del territorio, controlli su illeciti edilizia	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Soggetti richiedenti licenze o autorizzazioni amministrative

### CATEGORIA DATI:

CA

### TEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita

## PROGETTAZIONE, AFFIDAMENTO O ESECUZIONE DI OPERE PUBBLICHE

### DESCRIZIONE DEL TRATTAMENTO:

Progettazione, affidamento o esecuzione di opere pubbliche

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Progettazione, affidamento o esecuzione di opere pubbliche	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Lavoratori autonomi
Consulenti e liberi professionisti, anche in forma associata

### CATEGORIA DATI:

### CATEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## GARE E APPALTI

### DESCRIZIONE DEL TRATTAMENTO:

Il trattamento ha per oggetto le attività di gestione delle procedure ad evidenza pubblica che l'Ente pone in essere per individuare gli aggiudicatari dei contratti per la fornitura di beni e servizi. Comprende le attività specifiche di valutazione e comparazione delle offerte pervenute in accordo con le specifiche tecniche previste dai capitolati. I dati degli interessati verranno trattati in sede di valutazione delle offerte tecniche ed economiche e successivamente di aggiudicazione e stipula dei contratti. È possibile l'esecuzione di interrogazioni e incroci con altre banche dati a cui l'Amministrazione ha accesso, per raffronti con amministrazioni e gestori di pubblici servizi, finalizzate all'accertamento d'ufficio di uno stato, qualità o fatto ovvero al controllo a campione o massivo delle dichiarazioni sostitutive rese ai sensi dell'art. 43 del D.P.R. n. 445/2000

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Reclutamento e selezione del personale	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati relativi a condanne penali e reati; Lavoro; Istruzione e cultura; Idoneità al lavoro; Certificati di qualità professionali; Professione dichiarata; Dati di contatto (numero di telefono, e-mail, ecc.); Attività economiche, commerciali, finanziarie e assicurative; Coordinate bancarie; Certificati di qualità prodotti	Norma Stato membro (Decreto Legislativo 9 Aprile 2008 n.81)
Individuazione del miglior contraente	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati relativi a condanne penali e reati; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Istruzione e cultura; Attività economiche, commerciali, finanziarie e assicurative; Coordinate bancarie; Certificati di qualità	Norma Stato membro (Decreto Legislativo 9 Aprile 2008 n.81)



	professionali; Certificati di qualità prodotti; Professione dichiarata; Dati di contatto (numero di telefono, e-mail, ecc.); Idoneità al lavoro	
--	---	--

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Lavoratori autonomi
Candidati da considerare per l'instaurazione di un rapporto di lavoro
Consulenti e liberi professionisti, anche in forma associata
Fornitori

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale - Dati di contatto (numero di telefono, e-mail)	Dati comuni
Dati relativi a condanne penali e reati	Dati giudiziari
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Istruzione e cultura	Dati comuni
Attività economiche, commerciali, finanziarie e assicurative	Dati comuni
Idoneità al lavoro - Professione dichiarata	Dati relativi alla salute - Dati comuni
Coordinate bancarie	Dati comuni
Certificati di qualità professionali	Dati comuni
Certificati di qualità prodotti	Dati comuni

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## DIFESA DEL SUOLO

### DESCRIZIONE DEL TRATTAMENTO:

Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

### CATEGORIA DATI:

### CATEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## PROTEZIONE CIVILE

### DESCRIZIONE DEL TRATTAMENTO:

Protezione civile

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Protezione civile	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

### CATEGORIA DATI:

### CATEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## RISCOSSIONE IMPOSTE E TASSE COMUNALI

### DESCRIZIONE DEL TRATTAMENTO:

Riscossione Imposte e Tasse Comunali

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Riscossione Imposte e Tasse Comunali	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

### CATEGORIA DATI:

### CATEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita



## POLIZIA MUNICIPALE - VIDEOSORVEGLIANZA

### DESCRIZIONE DEL TRATTAMENTO:

Il trattamento ha per oggetto l'acquisizione di immagini e video attraverso un sistema di videosorveglianza, installato allo scopo di garantire la sicurezza della popolazione e la tutela del patrimonio dell'Ente.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Tutela del patrimonio dell'Ente	Immagini; Videoregistrazioni	GDPR
Sicurezza della popolazione	Immagini; Videoregistrazioni	GDPR
Sicurezza perimetrale, contro intrusioni e danneggiamento della proprietà dell'Ente	Immagini; Videoregistrazioni	GDPR

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Clienti o Utenti
Personale dipendente
Consulenti e liberi professionisti, anche in forma associata
Fornitori
Stagisti
Lavoratori somministrati

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Immagini	Dati comuni
Videoregistrazioni	Dati comuni/sensibili

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Massimo 7 giorni



## DIREZIONE ENTE LOCALE

### DESCRIZIONE DEL TRATTAMENTO:

Il trattamento ha per oggetto le attività di direzione generale dell'Ente, sotto le direttive e il coordinamento del Dirigente/Responsabile preposto alla specifica funzione, il quale adotta in autonomia i provvedimenti necessari al raggiungimento degli obiettivi fissati in sede di programmazione dagli organi politici e risponde dei risultati conseguiti. Questi in particolare predispone e sottoscrive gli atti gestionali di rilevanza interna ed esterna quali impegni di spesa, mandati di pagamento, reversali d'incasso, quelli relativi alle procedure di esperimento di gare, indizione di concorsi e ricopre solitamente il ruolo di presidenza nelle Commissioni di concorso e di gara.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Attività di direzione	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Attività economiche, commerciali, finanziarie e assicurative	
Stipula dei contratti	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Attività economiche, commerciali, finanziarie e assicurative	

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Personale dipendente - Contribuenti - Soggetti e/o organismi pubblici

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale - Nominativo, indirizzo o altri elementi di identificazione personale - Attività economiche, commerciali, finanziarie e assicurative	Dati comuni

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Adempimento di legge

## ANTICORRUZIONE E TRASPARENZA

### DESCRIZIONE DEL TRATTAMENTO:

Il trattamento ha per oggetto le attività a carico degli Enti Pubblici discendenti dalla normativa Anticorruzione (L. n. 190/2012) e Trasparenza (D.Lgs. 33/2013). Queste comprendono la predisposizione, approvazione e successivo aggiornamento del Piano Triennale di Prevenzione della Corruzione, la redazione della Relazione Annuale da parte del Responsabile per la Prevenzione della Corruzione, la pubblicazione dei dati e delle informazioni nella specifica sezione del sito internet istituzionale dell'Ente denominata Amministrazione Trasparente.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Adempimenti in materia di Anticorruzione	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati relativi a condanne penali e reati; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Istruzione e cultura; Lavoro; Dati relativi alla situazione reddituale	Norma Stato membro (Decreto Legislativo 9 Aprile 2008 n. 81)
Adempimenti in materia di Trasparenza	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati relativi a condanne penali e reati; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Istruzione e cultura; Lavoro; Dati relativi alla situazione reddituale	Norma Stato membro (Decreto Legislativo 9 Aprile 2008 n. 81)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:



INTERESSATI
Personale dipendente
Consulenti e liberi professionisti, anche in forma associata
Fornitori
Personale pubblico dirigenziale

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Codice fiscale ed altri numeri di identificazione personale	Dati comuni
Nominativo, indirizzo o altri elementi di identificazione personale	Dati comuni
Dati relativi a condanne penali e reati	Dati giudiziari
Lavoro (occupazione attuale, precedente, curriculum, ecc.)	Dati comuni
Istruzione e cultura	Dati comuni
Lavoro	Dati comuni
Dati relativi alla situazione reddituale	Dati comuni

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Adempimento di legge



## ATTIVITÀ RIGUARDANTE GLI ISTITUTI DI DEMOCRAZIA DIRETTA

### DESCRIZIONE DEL TRATTAMENTO:

Attività riguardante gli istituti di democrazia diretta

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	DATI TRATTATI	BASE GIURIDICA
Attività riguardante gli istituti di democrazia diretta	Categorie non definite	Norma Unione Europea (GDPR 2016/679)

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

### CATEGORIA DATI:

### CATEGORIE DI DESTINATARI:

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Trattamento a termine con data di scadenza non definita

## ATTIVITÀ DI SEGRETERIA GENERALE

### DESCRIZIONE DEL TRATTAMENTO:

Il trattamento riguarda i compiti che sono assegnati all'Ufficio dalla legge, dal regolamento sull'ordinamento degli uffici e dei servizi, e dal Sindaco. L'ufficio assiste inoltre gli organi di governo dell'ente nell'azione amministrativa assicurando il rispetto della legittimità dei provvedimenti.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Attività di Centralino Accoglimento dei visitatori Supporto amministrativo agli organi dell'Ente Attività di supporto al personale amministrativo Attività di direzione Attività di stipula dei contratti in nome e per conto dell'ente	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 - art. 6 del Reg. Ue 679/2016

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Soggetti a qualunque titolo interessati da rapporti con l'Ente

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Dati relativi alla situazione reddituale	Dati comuni
Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati comuni
Dati relativi ai carichi pendenti e al casellario giudiziale	Dati giudiziari

### CATEGORIE DI DESTINATARI:

Altre amministrazioni ed enti pubblici

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Adempimento di legge

## ECONOMATO, TRIBUTI ED ENTRATE COMUNALI

### DESCRIZIONE DEL TRATTAMENTO:

Il trattamento si occupa degli aspetti amministrativo-contabili di gestione dell'ente, compresa la gestione dei tributi locali.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Gestione tributi ed entrate comunali Gestione delle procedure sanzionatorie Attività relative al recupero evasione tributaria	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 - art. 6 del Reg. Ue 679/2016

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati comuni
Dati relativi ai carichi pendenti	Dati giudiziari

### CATEGORIE DI DESTINATARI:

Altre amministrazioni ed enti pubblici

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Adempimento di legge



## CONTROLLI EDILIZI

### DESCRIZIONE DEL TRATTAMENTO:

L'Ufficio svolge attività di: - Controlli edilizi, esame dei rapporti dei Vigili Urbani, sopralluoghi vari e attività amministrativa e sanzionatoria connessa (predispensione di ordinanze di sospensione dei lavori, di demolizione, adozione delle misure sanzionatorie per lavori abusivi etc.); - Ordinanze contingibili e urgenti in materia edilizia; - Esercizio di attività di consulenza nei confronti degli Organi del Comune per quanto attiene alle materie di competenza; - Verifiche per idoneità all'alloggio.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria Attività di verifica del rispetto della normativa di settore	Reg. UE 679/2016 - Regolamento Generale per la Protezione dei Dati Personali

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Imprenditori - Lavoratori autonomi - Cittadini - Soggetti richiedenti licenze e/o autorizzazioni amministrative

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati comuni
Dati relativi ai carichi pendenti	Dati giudiziari

*Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.*

### CATEGORIE DI DESTINATARI:

Altre amministrazioni ed enti pubblici

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Adempimento di legge



## URBANISTICA ED EDILIZIA

### DESCRIZIONE DEL TRATTAMENTO:

Il trattamento riguarda la tenuta e la gestione del Piano regolatore generale, degli strumenti urbanistici esecutivi, e di tutti gli atti di pianificazione territoriale. Rilascia i titoli a costruire, si interessa dell'agibilità delle costruzioni, certifica le destinazioni urbanistiche dei terreni, ed è l'ufficio destinatario a cui inoltrare i fascicoli edilizi.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Gestione delle pratiche relative ai progetti edilizi Gestione delle pratiche connesse all'abbattimento delle barriere architettoniche e all'agibilità di percorsi ed edifici Gestione delle pratiche relative alle istruttorie in materia urbanistica Gestione introiti oneri urbanizzazione Gestione delle pratiche relative ai permessi di costruire	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 - Reg. UE 679/2016 - Regolamento Generale per la Protezione dei Dati Personali

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini
Soggetti richiedenti licenze e/o autorizzazioni amministrative

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati comuni
Dati relativi ai carichi pendenti	Dati giudiziari

### CATEGORIE DI DESTINATARI:

Altre amministrazioni ed enti pubblici; In relazione ai Soggetti richiedenti licenze e/o autorizzazioni amministrative non sono previsti destinatari ai quali vengono comunicati i dati

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Adempimento di legge

## PUBBLICAZIONE ATTI ALL'ALBO PRETORIO

### DESCRIZIONE DEL TRATTAMENTO:

L'attività dell'albo pretorio consiste nella pubblicazione di tutti quegli atti sui quali viene apposto il "referto di pubblicazione": Deliberazioni, Ordinanze, Determinazioni, Avvisi, Manifesti, Gare, Concorsi e altri atti del Comune e di altri Enti pubblici, che devono essere portati a conoscenza del pubblico come atti emessi dalla Pubblica Amministrazione; Nel referto di pubblicazione viene indicato l'avviso di pubblicazione e di deposito dell'atto, con l'indicazione di chi l'ha emesso o adottato, l'oggetto, la data, il numero e la precisazione dell'ufficio presso il quale il documento e gli allegati sono consultabili.

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Attività di notifica, pubblicazione e deposito di atti, finalizzata a garantirne la conoscenza legale.	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

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini
Soggetti che interagiscono con l'Ente

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Non definibili	Dati comuni
Non definibili	Dati giudiziari
Non definibili	Dati sensibili

*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, inoltre deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.*

### CATEGORIE DI DESTINATARI: Non definibile

I termini previsti per la cancellazione: N/A

## SERVIZI CIMITERIALI

### DESCRIZIONE DEL TRATTAMENTO:

Attività di assegnazione di loculi, tombe ed aggiornamento dei registri

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Assegnazione di tombe e loculi	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

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini
Soggetti che interagiscono con l'Ente

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Non definibili	Dati comuni
Non definibili	Dati giudiziari
Non definibili	Dati sensibili

*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*

### CATEGORIE DI DESTINATARI:

In relazione al presente trattamento non sono previsti particolari destinatari ai quali vengono comunicati i dati

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Adempimento di legge

## NOTIFICAZIONE ATTI

### DESCRIZIONE DEL TRATTAMENTO:

Attività di notifica di atti, finalizzata a garantirne la conoscenza legale

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Attività di notifica, pubblicazione e deposito di atti, finalizzata a garantirne la conoscenza legale.	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

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

CATEGORIA DATO	TIPOLOGIA
Non definibili	Dati comuni

### CATEGORIE DI DESTINATARI:

Altre amministrazioni ed enti pubblici

I termini ultimi previsti per la cancellazione dei dati oggetto del trattamento sono determinati come segue: Adempimento di legge

## NUCLEO DI VALUTAZIONE

### DESCRIZIONE DEL TRATTAMENTO:

Dati trattati dall'O.I.V. o da organismo con funzioni analoghe

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Valutazione del personale dipendente interno all'Ente	Il trattamento è previsto da norma di legge

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Dipendenti dell'Ente

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Certificati di qualità professionali, Codice fiscale ed altri numeri di identificazione personale, Dati di contatto e comunicazione, Indirizzo e-mail, Nominativo, indirizzo o altri elementi di identificazione personale, Sesso m/f, Valutazione delle prestazioni professionali

### CATEGORIE DI DESTINATARI:

OdV, Dipendenti

Il trattamento avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti.

## RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD/DPO)

### DESCRIZIONE DEL TRATTAMENTO:

Dati trattati dal responsabile della protezione dei dati personali (RPD-DPO) in riferimento agli adempimenti previsti in materia di tutela e trattamento dei dati personali (privacy)

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Adempimento norme di legge (D.Lgs. 196/2003 – D.Lgs. 101/2018 – Reg. UE 679/2016)	Obblighi di legge; Il trattamento è necessario all'esecuzione di un contratto

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
N/A

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Codice fiscale ed altri numeri di identificazione personale, Contatto telefonico, Dati di contatto e comunicazione, Dati relativi alle immagini raccolti e trattati mediante sistemi di videosorveglianza, Indirizzo di residenza, Indirizzo e-mail, Nominativo, indirizzo o altri elementi di identificazione personale

### CATEGORIE DI DESTINATARI:

Data Protection Officer - Responsabile della Protezione dei Dati

I dati trasmessi ad eventuali fornitori di servizi esterni saranno da questi trattati per il tempo strettamente necessario all'esecuzione degli incarichi loro affidati e comunque avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti.

## SERVIZI FINANZIARI (Fornitori - Destinatari di pagamenti vari)

### DESCRIZIONE DEL TRATTAMENTO:

Dati relativi alle attività dei servizi finanziari comunali

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
1. Adempimento di obblighi fiscali e contabili 2. Gestione dei fornitori 3. Monitoraggio degli adempimenti contrattuali 4. Programmazione delle attività	Obbligo di legge; Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte e/o da norme di legge

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Dipendenti, Amministratori comunali, cittadini residenti, Aziende, liberi professionisti, delegati a presentare le istanze

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Attività economiche, commerciali, finanziarie e assicurative, Codice fiscale ed altri numeri di identificazione personale, Contatto telefonico, Dati fiscali e contabili, Indirizzo di residenza

### CATEGORIE DI DESTINATARI:

Enti locali, Banche e istituti di credito, Altre amministrazioni pubbliche, Agenzia delle Entrate

Il trattamento avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti.

## CONTRATTI E UFFICIO LEGALE

### DESCRIZIONE DEL TRATTAMENTO:

Attività contrattualistica e legale dell'Ente

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
1. Adempimento norme di legge; 2. Casi particolari: <i>Informazioni di carattere giudiziario</i>	Per le finalità 1: 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  Per le finalità 2: Consenso esplicito al trattamento

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Soggetti in rapporto contrattuale e legale con l'Ente

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Beni, proprietà, possesso, Certificati di qualità professionali, Codice fiscale ed altri numeri di identificazione personale, Contatto telefonico, Coordinate bancarie, Dati di contatto e comunicazione, Dati fiscali e contabili, Dati relativi al patrimonio immobiliare, Dati relativi alla famiglia o a situazioni personali, Indirizzo di residenza, Nominativo, indirizzo o altri elementi di identificazione personale, Sesso m/f

### CATEGORIE DI DESTINATARI:

Enti locali, Altre amministrazioni pubbliche, Agenzia delle Entrate

Il trattamento avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti.

## LAVORI PUBBLICI - MANUTENZIONI

### DESCRIZIONE DEL TRATTAMENTO:

Dati trattati per le procedure in materia di LL.PP. e manutenzioni

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Adempimento norme di legge; Motivi di interesse pubblico	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte e/o sulla base di norme di legge

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Artigiani, Imprenditori, Fornitori

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Attività economiche, commerciali, finanziarie e assicurative, Certificati di qualità professionali, Codice fiscale ed altri numeri di identificazione personale, Dati contabili, fiscali e finanziari, Dati inerenti situazioni giudiziarie civili, amministrative, tributarie, Nominativo, indirizzo o altri elementi di identificazione personale, Valutazione delle prestazioni professionali

### CATEGORIE DI DESTINATARI:

Enti locali, Altre amministrazioni pubbliche, Agenzia delle Entrate, altri Enti interessati

I dati verranno trattati per tutta la durata del rapporto contrattuale instaurato e anche successivamente per l'espletamento di tutti gli adempimenti di legge.



**POLIZIA MUNICIPALE/LOCALE - POLIZIA GIUDIZIARIA - VERBALI E  
SISTEMA SANZIONATORIO**

**DESCRIZIONE DEL TRATTAMENTO:**

Dati relativi alle attività di Polizia Locale

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Adempimento norme di legge; Motivi di interesse pubblico	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Minorenni, cittadini residenti, Persone non residenti presenti sul territorio

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Beni, proprietà, possesso, Codice fiscale ed altri numeri di identificazione personale, Dati di contatto e comunicazione, Dati relativi al patrimonio immobiliare, Dati relativi alla famiglia o a situazioni personali, Dati sul comportamento, Indirizzo di residenza, Nominativo, indirizzo o altri elementi di identificazione personale, Registrazioni filmati Videosorveglianza, Sesso m/f

**CATEGORIE DI DESTINATARI:**

Enti locali, Altre amministrazioni pubbliche, Agenzia delle Entrate, Autorità giudiziaria, altri Enti interessati

Il trattamento avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti e in base alle norme di legge.

## **RESPONSABILE DEL SERVIZIO DI PREVENZIONE E PROTEZIONE (RSPP)**

### DESCRIZIONE DEL TRATTAMENTO:

Dati trattati dal responsabile del servizio di prevenzione e protezione (RSPP) in materia di sicurezza sul luogo di lavoro e di medicina del lavoro

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Salute e sicurezza sul lavoro Motivi di interesse pubblico	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Dipendenti

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Codice fiscale ed altri numeri di identificazione personale, Contatto telefonico, Dati di contatto e comunicazione, Indirizzo e-mail, Nominativo, indirizzo o altri elementi di identificazione personale
1. Carte sanitarie 2. Idoneità al lavoro 3. Stato di salute 4. Stato di salute - patologie attuali

### CATEGORIE DI DESTINATARI:

N/A

I dati verranno conservati per il periodo strettamente necessario a garantire la corretta erogazione dei servizi acquistati

## SPORT, MANIFESTAZIONI E TURISMO

### DESCRIZIONE DEL TRATTAMENTO:

Organizzazione di manifestazioni e rapporti con le associazioni dei settori

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Attività associative e adempimento norme di legge	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 o per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini residenti, Associazioni e circoli

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Adesioni ad associazioni (esclusi partiti politici e soggetti sindacali), Nominativo, indirizzo o altri elementi di identificazione personale

### CATEGORIE DI DESTINATARI:

N/A

Il trattamento avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti.



## ORGANISMO DI DISCIPLINA

### DESCRIZIONE DEL TRATTAMENTO:

Dati trattati dall'organismo di disciplina ai sensi della vigente normativa, dei CCNL, del contratto decentrato e del Codice di disciplina

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Adempimento norme di legge Motivi di interesse pubblico	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Dipendenti

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Codice fiscale ed altri numeri di identificazione personale, Dati di contatto e comunicazione, Indirizzo di residenza, Sesso m/f, Valutazione delle prestazioni professionali
Informazioni di carattere giudiziario (in particolari casi)

### CATEGORIE DI DESTINATARI:

N/A

Il trattamento avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti

## SPORTELLO UNICO PER L'EDILIZIA

### DESCRIZIONE DEL TRATTAMENTO:

Attività del SUE in materia di edilizia privata

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Adempimento norme di legge	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 Dati forniti sulla base di consenso esplicito in rari casi

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Cittadini residenti e non, professionisti abilitati a presentare istanze

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Beni, proprietà, possesso, Certificati di qualità professionali, Codice fiscale ed altri numeri di identificazione personale, Coordinate bancarie, Dati di contatto e comunicazione, Dati relativi al patrimonio immobiliare, Indirizzo di residenza, Professione dichiarata, Sesso m/f Stato di salute: possibile trattamento di dati relativi alla salute per pratiche edilizie relative all'accesso ai disabili

### CATEGORIE DI DESTINATARI:

Enti locali, Consulenti e liberi professionisti anche in forma associata, Altre amministrazioni pubbliche, ASL, Aziende ospedaliere e Regioni, Camere di commercio, industria, artigianato ed agricoltura, Agenzia delle entrate, Soggetti privati (persone fisiche o giuridiche)

Il trattamento avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti

## SPORTELLO UNICO PER LE ATTIVITÀ PRODUTTIVE

### DESCRIZIONE DEL TRATTAMENTO:

Attività di SUAP

I dati personali oggetto del trattamento sono raccolti e trattati per le finalità riportate di seguito insieme alla base giuridica di riferimento:

FINALITÀ	BASE GIURIDICA
Adempimento norme di legge Motivi di interesse pubblico	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento

I dati personali raccolti afferiscono alle categorie di interessati la cui descrizione è riportata di seguito:

INTERESSATI
Aziende, liberi professionisti, delegati a presentare le istanze

I dati personali raccolti afferiscono alle categorie la cui descrizione è riportata di seguito:

DATI TRATTATI
Attività economiche, commerciali, finanziarie e assicurative, Beni, proprietà, possesso, Certificati di qualità prodotti, Certificati di qualità professionali, Codice fiscale ed altri numeri di identificazione personale, Dati di contatto e comunicazione, Dati relativi al patrimonio immobiliare, Indirizzo di residenza, Nominativo, indirizzo o altri elementi di identificazione personale, Professione dichiarata
Informazioni di carattere giudiziario

### CATEGORIE DI DESTINATARI:

Enti locali, Altre amministrazioni pubbliche, ASL, Aziende ospedaliere e Regioni, Autorità giudiziaria, Camere di commercio, industria, artigianato ed agricoltura, Soggetti privati (persone fisiche o giuridiche)

Il trattamento avrà una durata non superiore a quella necessaria alle finalità per le quali i dati sono stati raccolti



## CONSERVAZIONE DEI DATI

INTERESSATI	CATEGORIE DI DATI	DURATA CONSERVAZIONE	Principali Riferimenti Normativi
Soggetti portatori di handicap	Dati idonei a rivelare le convinzioni religiose	10 anni	
	Stato di salute - patologie attuali	10 anni	
	Stato di salute - anamnesi familiare	10 anni	
	Dati idonei a rivelare le convinzioni filosofiche	10 anni	
	Stato di salute - terapie in corso	10 anni	
	Stato di salute - patologie pregresse	10 anni	
	Dati idonei a rivelare l'origine razziale ed etnica	10 anni	
Soggetti che versano in condizioni di indigenza	Dati giudiziari	10 anni	
	Stato di salute - patologie attuali	10 anni	
	Stato di salute - relativo a familiari	10 anni	
	Dati sanitari dell'interessato relative ai familiari	10 anni	
	Stato di salute - terapie in corso	10 anni	
	Stato di salute - patologie pregresse	10 anni	
	Dati idonei a rivelare l'origine razziale ed etnica	10 anni	
Soggetti bisognosi di assistenza domiciliare e di aiuti di carattere socio- assistenziale	Stato di salute - patologie attuali	10 anni	
	Stato di salute - relativo a familiari	10 anni	
	Stato di salute - terapie in corso	10 anni	
	Stato di salute - patologie pregresse	10 anni	
Iscritti o candidati a partiti politici o liste civiche	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Illimitato	
	Dati idonei a rivelare l'adesione a partiti	Illimitato	
Soggetti in stato di non autosufficienza psico-fisica	Dati giudiziari	10 anni	
	Dati idonei a rivelare le convinzioni religiose	10 anni	
	Stato di salute - patologie attuali	10 anni	
	Stato di salute - anamnesi familiare	10 anni	



	Dati idonei a rivelare le convinzioni filosofiche	10 anni	
	Stato di salute - terapie in corso	10 anni	
	Stato di salute - patologie pregresse	10 anni	
	Dati idonei a rivelare l'origine razziale ed etnica	10 anni	
Utenti	Dati idonei a rivelare le convinzioni religiose	10 anni	
	Stato di salute - patologie attuali	10 anni	
	Dati idonei a rivelare le convinzioni filosofiche	10 anni	
	Dati idonei a rivelare le opinioni politiche	10 anni	
	Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche es. convinzioni alimentari)	10 anni	
Imprenditori	Dati giudiziari	10 anni	
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni	
	Dati di contatto (numero di telefono, e-mail, ecc.)	10 anni	
Commercianti	Dati giudiziari	10 anni	
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni	
Collaboratori	Dati idonei a rivelare l'adesione a sindacati	10 anni	
	Curriculum Vitae	10 anni	
	Dati relativi all'esperienza professionale	10 anni	
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni	
	Dati idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	10 anni	
	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche	10 anni	



	Dati di contatto (numero di telefono, e-mail, ecc.)	10 anni	
	Dati giudiziari	10 anni	
	Stato di salute - patologie attuali	10 anni	
Soggetti a qualunque titolo interessati da rapporti con l'Ente	Dati giudiziari	10 anni	
	Dati personali idonei a rivelare lo stato di salute	10 anni	
	Dati relativi alla situazione reddituale	10 anni	
	Dati personali idonei a rivelare la vita sessuale	10 anni	
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni	
	Dati relativi ai carichi pendenti e al casellario giudiziale	10 anni	
	Dati idonei a rivelare l'origine nazionale	10 anni	
	Dati idonei a rivelare l'origine razziale ed etnica	10 anni	
	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche	10 anni	
	Impronte digitali	10 anni	
Soggetti coinvolti in violazioni in materia sanitaria o ambientale	Dati giudiziari	10 anni	
	Stato di salute - patologie attuali	10 anni	
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni	
Lavoratori autonomi	Dati giudiziari	10 anni	
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni	
Soggetti minorenni	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni	
	Dati idonei a rivelare il rapporto di parentela	10 anni	
	Dati idonei a rivelare lo stato di disabilità	10 anni	
	Categoria particolari di dati	10 anni	
	Dati idonei a rivelare l'adesione alla profilassi vaccinale obbligatoria	10 anni	



	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche	10 anni	
Cittadini	Dati giudiziari	Illimitatamente	
	Dati personali idonei a rivelare lo stato di salute	Illimitatamente	
	Dati idonei a rivelare le convinzioni religiose	Illimitatamente	
	Stato di salute - patologie attuali	Illimitatamente	
	Dati personali idonei a rivelare la vita sessuale	Illimitatamente	
	Dati Biometrici	Illimitatamente	
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Illimitatamente	
	Stato di salute - relativo a familiari	Illimitatamente	
	Dati relativi ai carichi pendenti e al casellario giudiziale	Illimitatamente	
	Dati relativi ad altri provvedimenti o procedimenti giudiziari	Illimitatamente	
	Categoria particolari di dati	Illimitatamente	
	Stato di salute - terapie in corso	Illimitatamente	
	Stato di salute - patologie pregresse	Illimitatamente	
	Dati idonei a rivelare l'origine razziale ed etnica	Illimitatamente	
	Dati relativi alla situazione reddituale (busta paga, CUD, cedolino pensione, ecc.)	Illimitatamente	
	Dati di contatto (numero di telefono, e-mail, ecc.)	Illimitatamente	
Soggetti in stato di disagio sociale	Dati idonei a rivelare le convinzioni religiose	10 anni	
	Stato di salute - patologie attuali	10 anni	
	Stato di salute - terapie in corso	10 anni	
	Stato di salute - patologie pregresse	10 anni	
	Dati idonei a rivelare l'origine razziale ed etnica	10 anni	
Personale impiegato a vario titolo	Stato di salute - patologie attuali	10 anni	
	Stato di salute - terapie in corso	10 anni	



	Stato di salute - patologie pregresse	10 anni	
Soggetti coinvolti in incidenti e/o infortuni stradali	Stato di salute - patologie attuali	N/A	
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	N/A	
	Stato di salute - terapie in corso	N/A	
Soggetti richiedenti licenze o autorizzazioni amministrative	Dati giudiziari	Illimitatamente	
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Illimitatamente	

# Map Results

July 20, 2018

This report was generated with an evaluation version of Qualys

## Report Summary

User Name:	Antonio Leo
Login Name:	ctegr5al2
Company:	Citel Group
User Role:	Manager
Address:	Via Giovanni Porzio 101
City:	Napoli
Zip:	80143
Country:	Italy
Created:	07/20/2018 at 12:40:37 (GMT+0200)
Sort by:	IP Address
Domain:	none:[192.168.50.1-192.168.50.234, 192.168.50.238-192.168.50.254]
Map:	
Type:	On demand
Status:	Finished
Title:	asset inventory map
Date:	2018-07-09 12:39:46
Reference:	map/1531139881.24062
Duration:	00:03:46
Total Hosts Found:	34
Scanner Appliance:	MonteDiProcida (Scanner 10.1.31-1, Vulnerability Signatures 2.4.368-2)
Option Profile:	Initial Options

none:[192.168.50.1-192.168.50.234, 192.168.50.238-192.168.50.254](34)

IP	DNS	NetBIOS	Router	OS	Approved	Scannable	Live	Netblock
192.168.50.1	SERVER01			Windows 2003		S	L	N
Discovery Method   Port								
ICMP								
TCP	53							
TCP	80							
TCP	88							
TCP	135							
TCP	139							
TCP	445							
UDP	53							
UDP	137							
TCP RST								
192.168.50.2	SERVER02			Windows 2003		S	L	N
Discovery Method   Port								
ICMP								
TCP	80							
TCP	135							
TCP	139							
TCP	445							
UDP	137							
TCP RST								

IP	DNS	NetBIOS	Router	OS	Approved	Scannable	Live	Netblock
192.168.50.3	SERVER03			Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10		S	L	N
Discovery Method	Port							
ICMP								
TCP	80							
TCP	135							
TCP	139							
TCP	445							
UDP	137							
TCP RST								
192.168.50.4	SERVER04			Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10		S	L	N
Discovery Method	Port							
ICMP								
TCP	80							
TCP	135							
TCP	139							
TCP	443							
TCP	445							
UDP	137							
TCP RST								
192.168.50.5	PROTOCOLLO			Windows 2008 R2 / Windows 7		S	L	N
Discovery Method	Port							
TCP	80							
TCP	135							
TCP	139							
TCP	445							
UDP	137							
ICMP								
192.168.50.6	MARIO2			Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10		S	L	N
Discovery Method	Port							
ICMP								
TCP	135							
TCP	139							
TCP	445							
UDP	137							
192.168.50.13	SERVER2			Windows 2000 Service Pack 3-4		S	L	N
Discovery Method	Port							
ICMP								
TCP	135							
TCP	139							
TCP	445							
UDP	137							
TCP RST								
192.168.50.15	PCGIOV			Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10		S	L	N
Discovery Method	Port							
ICMP								
TCP	135							
TCP	139							
TCP	445							
UDP	137							
192.168.50.20				Cisco ASA Firewall		S	L	N
Discovery Method	Port							
ICMP								
TCP	443							
TCP RST								

IP	DNS	NetBIOS	Router	OS	Approved	Scannable	Live	Netblock
192.168.50.21	UTC-3			Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10		S	L	N
Discovery Method	Port							
ICMP								
TCP	135							
TCP	139							
TCP	445							
UDP	137							
192.168.50.25	SERVIZISOCIALI			Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10		S	L	N
Discovery Method	Port							
ICMP								
TCP	135							
TCP	139							
TCP	445							
UDP	137							
192.168.50.29	N4310			Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP		S	L	N
Discovery Method	Port							
ICMP								
TCP	80							
TCP	111							
TCP	139							
TCP	443							
TCP	445							
UDP	111							
UDP	137							
TCP RST								
192.168.50.30	RAGCOM3X			Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10		S	L	N
Discovery Method	Port							
TCP	135							
TCP	139							
TCP	445							
UDP	137							
ICMP								
192.168.50.35	UTCTOBIA			Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10		S	L	N
Discovery Method	Port							
ICMP								
TCP	135							
TCP	139							
TCP	445							
UDP	137							
192.168.50.37	DESKTOP-SINDA CO			Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10		S	L	N
Discovery Method	Port							
ICMP								
TCP	135							
TCP	139							
TCP	445							
UDP	137							
192.168.50.38	TRIBUTI			Windows 2003/XP		S	L	N
Discovery Method	Port							
ICMP								
TCP	135							
TCP	139							
TCP	445							
UDP	137							

IP	DNS	NetBIOS	Router	OS	Approved	Scannable	Live	Netblock
192.168.50.39	ZSD			Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10		S	L	N
Discovery Method	Port							
ICMP								
TCP	135							
TCP	139							
TCP	445							
UDP	137							
192.168.50.77	BRN3C2AF41E15 BD			Unknown / Brother Printer		S	L	N
Discovery Method	Port							
ICMP								
TCP	25							
TCP	80							
TCP	443							
UDP	137							
TCP RST								
192.168.50.78	BRN3C2AF41E15 AD			Unknown / Brother Printer		S	L	N
Discovery Method	Port							
ICMP								
TCP	25							
TCP	80							
TCP	443							
UDP	137							
TCP RST								
192.168.50.79	BRN3C2AF41E15 BF			Unknown / Brother Printer		S	L	N
Discovery Method	Port							
ICMP								
TCP	25							
TCP	80							
TCP	443							
UDP	137							
TCP RST								
192.168.50.80	BRN3C2AF41E15B 2			Unknown / Brother Printer		S	L	N
Discovery Method	Port							
ICMP								
TCP	25							
TCP	80							
TCP	443							
UDP	137							
TCP RST								
192.168.50.81	BRN3C2AF41E171 9			Unknown / Brother Printer		S	L	N
Discovery Method	Port							
ICMP								
TCP	25							
TCP	80							
TCP	443							
UDP	137							
TCP RST								
192.168.50.82	BRN3C2AF41E15 C2			Unknown / Brother Printer		S	L	N
Discovery Method	Port							
ICMP								
TCP	25							
TCP	80							
TCP	443							
UDP	137							

TCP RST

192.168.50.95	SETTOREXIII	Windows 2003/XP	S	L	N
Discovery Method	Port				
ICMP					
TCP	135				
TCP	139				
TCP	445				
UDP	137				
192.168.50.96	ASSESSORI-PC	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10	S	L	N
Discovery Method	Port				
ICMP					
TCP	135				
TCP	139				
TCP	445				
UDP	137				
192.168.50.120	AVVOCATURA	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10	S	L	N
Discovery Method	Port				
ICMP					
TCP	135				
TCP	139				
TCP	445				
UDP	137				
192.168.50.161		Cisco Firewall Services Module	S	L	N
Discovery Method	Port				
ICMP					
TCP	22				
TCP	23				
TCP	443				
UDP	53				
TCP RST					
192.168.50.221	COMANDO2	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10	S	L	N
Discovery Method	Port				
ICMP					
TCP	135				
TCP	139				
TCP	445				
UDP	137				
192.168.50.222	COMANDANTE	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10	S	L	N
Discovery Method	Port				
ICMP					
TCP	135				
TCP	139				
TCP	445				
UDP	137				
192.168.50.224	COMANDO1	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10	S	L	N
Discovery Method	Port				
ICMP					
TCP	135				
TCP	139				
TCP	445				
UDP	137				
192.168.50.226	COMANDO3	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10	S	L	N
Discovery Method	Port				
ICMP					

TCP	135
TCP	139
TCP	445
UDP	137

192.168.50.227	Windows 2003	S	L	N
Discovery Method	Port			
ICMP				
TCP	21			
TCP	80			
TCP	135			
TCP	445			
TCP RST				

192.168.50.228	Windows 2003	S	L	N
Discovery Method	Port			
TCP	135			
TCP	445			

192.168.50.231		S	L	N
Discovery Method	Port			
ICMP				
TCP RST				

## Appendix

Legend	
A:	Approved
S:	Scannable
L:	Live
N:	In Netblock

## Option Profiles

Initial Options	
Basic Information Gathering: All Hosts	
TCP Ports:	Standard Scan
UDP Ports:	Standard Scan
Live Host Sweep:	On
Disable DNS traffic:	Off
Authenticated Scans:	None
Overall Performance:	Normal
Netblocks to Map in Parallel:	
External Scanners:	6
Scanner Appliances:	8
Netblock Size:	16384 IPs
Packet (Burst) Delay:	Minimum

This report was generated with an evaluation version of Qualys

### CONFIDENTIAL AND PROPRIETARY INFORMATION.

Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2018, Qualys, Inc.

The background of the slide is a dark red color. Overlaid on this is a complex, abstract network of thin, light red lines connecting numerous small, glowing red dots. These dots and lines are scattered across the entire frame, creating a sense of a global or digital network. The lines vary in length and thickness, and the dots are of varying sizes and brightness.

# **REPORT DI VALUTAZIONE DELLE MINACCE INFORMATICHE**

# Statistiche vitali

Questo documento illustra i risultati prodotti da una recente analisi della vostra infrastruttura. Si tratta infatti di una sintesi delle conclusioni a cui è giunta la valutazione e dei suggerimenti utili per affrontare gli eventi rilevati. Di seguito le specifiche dell'analisi dei dati raccolti:

## Dettagli dell'azienda presa in esame

**Nome azienda:** Comune di Monte di Procida

**Località:** Monte di Procida (NA), IT

**Settore:** Government

**Dimensioni:** 25-99 employees

## Dettagli del test

**Dati di inizio:** Jul 13, 2018

**Durata:** 15 Giorno/i

**Modello FortiGate:** FG-100D

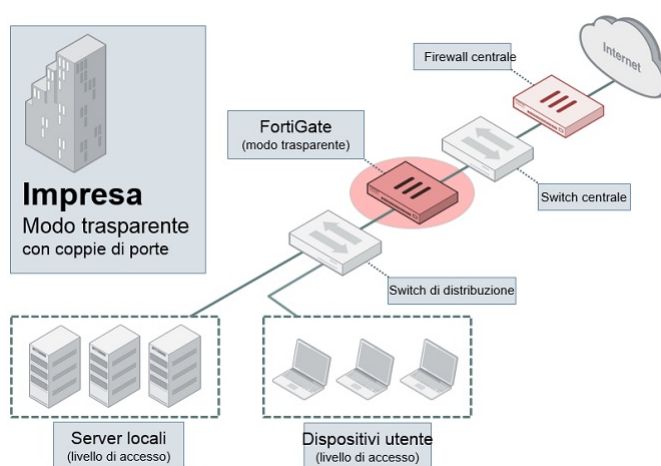
**Firmware FortiOS:** FortiOS 5.6.2

**Rete analizzata:** Internal LAN

**Funzioni abilitate:** Firewall

## Distribuzione e metodologia

La rete è stata monitorata con un FG-100D in modalità Transparent Mode (Port Pair). Si tratta di un sistema non invasivo per intercettare il traffico durante il transito in rete.



La valutazione ha preso in esame l'attività di rete durante il passaggio attraverso l'infrastruttura. Sebbene i log del traffico registrino gran parte delle informazioni sulle sessioni per l'intera rete, i FortiGate possono monitorare anche i processi di registrazione operativi a un livello più profondo, come quelli concernenti l'IPS, l'antivirus, la verifica Web e l'Application Control. L'analisi si fonda sulla telemetria di dati provenienti da ogni tipo di log e offre una panoramica dell'attività di rete. Se abbinati a FortiAnalyzer, i FortiGate sono in grado di eseguire ulteriori funzioni come la gestione degli eventi (ad es. gli avvisi), l'analisi con gli strumenti FortiView (ad es. indagini su specifiche attività degli utenti) e il reporting.

# Sintesi preliminare



## Sicurezza e prevenzione delle minacce

**Attacchi IPS rilevati:** 117,806

**Malware/botnet rilevati:** 0

**Applicazioni ad alto rischio utilizzate:** 13

**Siti Web malevoli rilevati:** 17

L'anno scorso, oltre 2.100 imprese hanno subito violazioni dovute alla scarsa qualità della sicurezza interna e alla latenza della content security dei vari fornitori. Si stima che il costo medio di una violazione si aggiri intorno ai 3,5 milioni di dollari USA e che cresca del 15% ogni anno. Intrusioni, malware/botnet e applicazioni malevoli sono un enorme rischio per le reti aziendali. Questi meccanismi di attacco consentono ai cybercriminali di accedere ai database e ai file più riservati. FortiGuard Labs attenua i pericoli con un pluripremiato sistema di content security che le è valso il massimo apprezzamento di società di test indipendenti, quali NSS Labs, VB 100 e AV Comparatives.



## Produttività dell'utente

**Applicazioni rilevate:** 238

**Principale applicazione utilizzata:** HTTPS.BROWSER

**Principale categoria applicativa:** Web.Client

**Siti Web visitati:** 11,822

**Principale sito Web:** update.eset.com

**Principale categoria Web:** Information Technology

L'uso delle applicazioni e le abitudini di navigazione degli utenti indicano non solo un impiego inefficiente delle risorse ma anche la mancanza di un'adeguata conformità alle policy aziendali. Le imprese ritengono accettabile che le risorse siano adoperate per scopi personali, ma hanno molte le aree grigie da controllare: le applicazioni peer-to-peer/per l'elusione proxy, l'inappropriata navigazione sul Web, i siti Web di phishing e le attività illecite; tutti pericoli che espongono a responsabilità e danni. Con più di 5.800 regole di Application Control e 250 milioni di siti Web classificati, FortiGuard Labs offre le funzioni di telemetria che FortiOS usa per l'operatività del business.



## Utilizzo delle Rete

**Larghezza di banda totale:** 97.07 GB

**Host principale per larghezza di banda:**  
192.168.50.248

**Host con il numero di sessioni più elevato:**  
192.168.50.248

**Intervallo di registrazione medio/sec.:** 12.37

Le prestazioni sono spesso sottovalutate, ma i firewall sostengono le velocità di linea degli switch di nuova generazione. Per Infonetics, il 77% delle aziende ritiene che sia necessario passare a un throughput di oltre 100 Gbps. I FortiGate usano FortiASIC per accelerare l'inoltro di pacchetti e il pattern matching, con prestazioni decuplicate rispetto alla concorrenza.

# Azioni consigliate

## Attacchi alle vulnerabilità applicative rilevati ( 107 )

Le vulnerabilità applicative (prese di mira dagli attacchi IPS) fungono da punti di ingresso per bypassare l'infrastruttura di sicurezza e permettono agli aggressori di introdursi nell'organizzazione. Vengono spesso sfruttate a causa di mancati aggiornamenti o per l'assenza di un processo di gestione delle patch. Per proteggersi da attacchi a carico delle vulnerabilità applicative è essenziale identificare eventuali host privi di patch.

## Malware rilevati ( 0 )

I malware possono assumere molteplici forme e presentarsi nelle vesti di virus, trojan, spyware/adware e così via. Se viene rilevato malware in rete è possibile che sia presente un vettore di attacco che ha origine, probabilmente inconsapevole, all'interno dell'organizzazione stessa. L'analisi combinata di signature e comportamenti riesce di norma a impedire l'esecuzione di malware e la conseguente esposizione della rete ad attività malevoli. Se si potenzia l'ambiente con tecnologie APT/sandbox (come FortiSandbox), è possibile anche impedire la propagazione di malware noti (minacce zero-day).

## Infezioni da botnet ( 0 )

I bot possono essere adoperati per lanciare attacchi DoS (Denial-of-Service), diffondere spam, spyware e adware, propagare codice malevole e acquisire informazioni sensibili, con conseguenze finanziarie e legali anche molto gravi. Le infezioni da botnet devono essere prese sul serio e affrontate con azioni immediate. Occorre identificare quanto prima i computer compromessi e ripulirli con l'ausilio di software antivirus. Il sistema FortiClient di Fortinet consente di analizzare l'ambiente e rimuovere le botnet dagli host infetti.

## Siti Web malevoli rilevati ( 17 )

Per siti Web malevoli si intendono quegli spazi online che ospitano software/malware concepiti per raccogliere informazioni di nascosto, danneggiare il computer host o manipolare in altro modo la macchina bersaglio senza il consenso dell'utente. La visita di uno di tali siti precede in genere l'infezione e rappresenta la fase iniziale della catena di attacco. La strategia di prevenzione migliore in questi casi è bloccare i siti malevoli e/o istruire i dipendenti di non visitarli né di installare software proveniente da fonti sconosciute.

## Siti Web di phishing rilevati ( 6 )

Analogamente ai siti Web malevoli, i siti di phishing emulano le pagine di siti Web leciti nel tentativo di raccogliere informazioni personali o riservate (login, password, ecc.) degli utenti finali. Ad essi si accede spesso tramite link presenti in email non richieste inviate ai dipendenti. Per evitare attacchi di phishing è utile assumere un atteggiamento scettico nei confronti delle email che richiedono informazioni personali e indagare sulla validità dei link.

## Applicazioni proxy rilevate ( 6 )

Queste applicazioni vengono utilizzate (generalmente in maniera intenzionale) per bypassare le misure di sicurezza applicate. Può accadere, ad esempio, che gli utenti aggirino il firewall camuffando o criptando le comunicazioni esterne. In molti casi, questo può essere considerato un atto doloso e una vera e propria violazione delle policy d'uso aziendali.

## Applicazioni di accesso remoto rilevate ( 7 )

Le applicazioni di accesso remoto vengono spesso impiegate per accedere a distanza ad host interni, aggirando così il sistema NAT o tracciando un percorso di accesso secondario (backdoor) agli host interni. Nei casi peggiori, l'accesso remoto può servire a favorire l'esfiltrazione dei dati e lo spionaggio industriale. Se, come spesso capita, non ci sono restrizioni a questo tipo di accesso, occorre modificare le prassi aziendali interne perché siano previste limitazioni in tal senso.

## Applicazioni P2P e di condivisione file ( 2 )

Queste applicazioni richiedono l'uso di policy di regolamentazione poiché possono essere usate per bypassare i controlli dei contenuti ed eseguire trasferimenti di dati non autorizzati o violazioni.

# Sicurezza e prevenzione delle minacce

## Applicazioni ad alto rischio

Il team di ricerca FortiGuard assegna un rating da 1 a 5 per classificare il rischio associato ad un'applicazione sulla base di caratteristiche comportamentali della stessa. Questo tipo di classificazione consente agli amministratori di identificare rapidamente le applicazioni ad alto rischio e di prendere decisioni più oculate sulle policy di Application Control. Alle applicazioni elencate in basso è stato assegnato un livello di rischio pari o superiore a 4.

### Applicazioni ad alto rischio

#	Rischio	Nome applicazione	Categoria	Tecnologia	Utenti	Larghezza di banda	Sessioni
1	5	Proxy.HTTP	Proxy	Network-Protocol	2	813.54 KB	176
2	5	SOCKS4	Proxy	Network-Protocol	1	6.12 KB	36
3	5	SOCKS5	Proxy	Network-Protocol	1	3.38 KB	18
4	5	Proxy.Websites	Proxy	Browser-Based	2	4.85 KB	3
5	4	Telnet	Remote.Access	Client-Server	822	7.96 MB	7,116
6	4	BitTorrent	P2P	Peer-to-Peer	2	1,003.31 KB	1,320
7	4	TeamViewer	Remote.Access	Client-Server	9	374.76 MB	1,238
8	4	Citrix.Receiver	Remote.Access	Client-Server	2	71.34 KB	200
9	4	RDP	Remote.Access	Client-Server	2	7.33 KB	37
10	4	Gnutella	P2P	Peer-to-Peer	1	7.45 KB	36

Figura 1: applicazioni a più alto rischio ordinate in base al grado di rischio e alle sessioni

## Exploit delle vulnerabilità applicative

Le vulnerabilità applicative possono essere sfruttate per compromettere la sicurezza della rete. Il team di ricerca FortiGuard analizza queste vulnerabilità e sviluppa quindi signature per rilevarle. FortiGuard adopera attualmente un database di oltre 5.800 minacce applicative note, per rilevare attacchi che eludono i tradizionali sistemi firewall. Ulteriori informazioni sulle vulnerabilità applicative sono disponibili sul sito Web FortiGuard all'indirizzo: <http://www.fortiguard.com/intrusion>.

### Principali exploit di vulnerabilità applicative rilevati

#	Gravità	Nome minaccia	Tipo	Vittime	Fonte	Numero
1	5	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	1	1	266
2	5	Apache.Struts.2.REST.Plugin.Remote.Code.Execution	Code Injection	1	1	168
3	5	Cisco.IOS.HTTP.Command.Execution	Improper Authentication	1	1	42
4	5	Necurs.Botnet		1	1	28
5	5	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	1	1	24
6	5	Adobe.Coldfusion.BlazeDS.Java.Object.Deserialization	Code Injection	1	1	14
7	5	Apache.Commons.Collection.InvokerTransformer.Code.Execution	OS Command Injection	1	1	14
8	5	Accellion.FTA.Cookie.Information.Disclosure	Information Disclosure	1	1	14
9	5	MS.IIS.WebHits.Authentication.Bypass	Improper Authentication	1	1	14
10	5	SWEditServlet.DirectoryTraversal	Path Traversal	1	1	14

Figura 2: principali vulnerabilità identificate, ordinate per livello di gravità e numero

## Malware, botnet e spyware/adware

Sono molti i canali che i cybercriminali utilizzano per distribuire malware. La procedura più comune consiste nell'indurre gli utenti ad aprire un file infetto presente in un allegato di posta elettronica, scaricare un file infetto o fare clic su un link che indirizza a un sito malevole. Durante la valutazione della sicurezza, Fortinet ha identificato diversi eventi correlati a malware e botnet che indicano download di file malevoli o connessioni a siti di Command&Control (C&C) di botnet.

### Principali malware, botnet e spyware/adware rilevati

No matching log data for this report

Figura 3: malware, botnet, spyware e adware più comuni rilevati

## Dispositivi e host a rischio

Sulla base dei tipi di attività presenti su un host, è possibile valutare l'attendibilità di ogni singolo client. La reputazione del client dipende da fattori essenziali quali i siti Web visitati, le applicazioni adoperate e le destinazioni in entrata/in uscita utilizzate. A conclusione della verifica è possibile generare un punteggio complessivo delle minacce esaminando l'attività aggregata di ogni singolo host.

### Dispositivi e host più a rischio

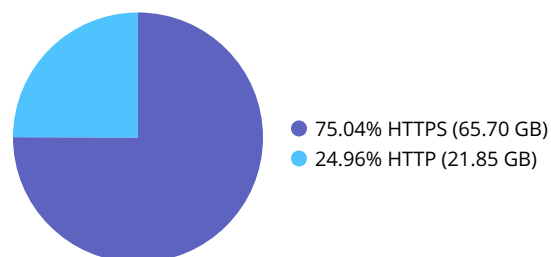
#	Dispositivo	Punteggio
1	192.168.50.235	625,515
2	192.168.50.249	21,125
3	SERVIZISOCIALI	20,565
4	192.168.50.248	14,325
5	SCENIC	13,620
6	192.168.50.227	10,345
7	TRIBUTI	8,625
8	MONTEDIPROCIDA	5,000
9	COMANDO1	1,955
10	ARCHILLIANO	1,175

Figura 4: è consigliabile controllare questi dispositivi per valutarne la ricettività nei confronti di malware e intrusioni

## Traffico Web criptato

Nell'ottica della sicurezza, è importante capire quanto traffico Web sia criptato. Il traffico criptato crea seri problemi per le aziende che desiderano assicurare che le applicazioni in questione non vengano adoperate per scopi dolosi, inclusa l'esfiltrazione di dati. L'ideale sarebbe che il firewall fosse in grado di ispezionare il traffico criptato ad elevate velocità. Ecco perché le performance e l'offload di hardware/ASIC sono fondamentali per la valutazione di una soluzione.

### Rapporto tra traffico HTTPS e HTTP



## Principali paesi di origine

Esaminando il traffico sorgente IP è possibile risalire al paese di origine di una determinata richiesta. Botnet, funzioni di Command&Control e persino accessi remoti possono richiedere molte sessioni e celare attacchi mirati o minacce persistenti provenienti da stati nazione. La tabella che segue riporta il traffico che si origina in determinati paesi, poiché le attività provenienti da specifiche nazioni può risultare anomala e richiedere ulteriori indagini.

### Principali paesi di origine

#	Paese	Larghezza di banda
1	China	2.54 MB
2	United States	1.04 MB
3	Russian Federation	627.56 KB
4	Vietnam	485.33 KB
5	Korea, Republic of	368.47 KB
6	Italy	283.64 KB
7	Egypt	271.68 KB
8	Turkey	271.62 KB
9	Hong Kong	238.81 KB
10	Sweden	220.53 KB

Figura 5: è consigliabile controllare le attività provenienti da questi paesi per individuare eventuali fonti di traffico previste

# Produttività dell'utente

## Uso delle applicazioni

Il team di ricerca FortiGuard ascrive le applicazioni a diverse categorie sulla base di caratteristiche comportamentali, tecnologia sottostante e peculiarità delle transazioni di traffico correlate. Le categorie permettono un maggiore Application Control. FortiGuard gestisce migliaia di sensori applicativi e può persino eseguire ispezioni approfondite sulle applicazioni, consentendo, ad esempio, ai responsabili IT di ottenere una visibilità senza precedenti sui nomi dei file inviati al cloud o sui titoli dei video riprodotti in streaming.

Per informazioni dettagliate sulle categorie di applicazioni, consultate la pagina al seguente indirizzo:

<http://www.fortiguard.com/encyclopedia/application>

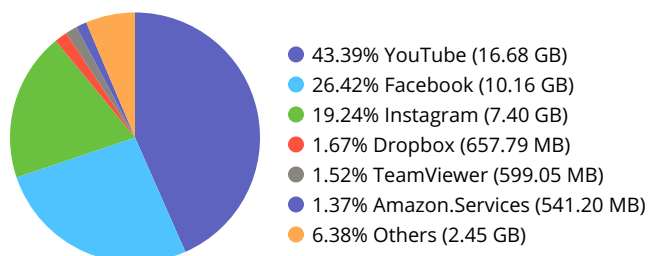
### Categorie di app

Web.Client	28.66%
Social.Media	18.34%
Video/Audio	17.86%
Update	15.15%
General.Interest	9.01%
Email	2.47%
Network.Service	2.38%
Collaboration	1.65%
Unknown	1.32%
Storage.Backup	1.21%
Others	1.96%



Con il massiccio impiego dell'elaborazione cloud, le imprese si affidano sempre di più a terze parti per la predisposizione dell'infrastruttura. Sfortunatamente però questo significa che le loro informazioni saranno sicure solo nella misura in cui sono sicuri i servizi del fornitore del cloud. Inoltre, se i servizi sono già disponibili internamente, si producono ridondanze, e se invece il monitoraggio non avviene correttamente, aumentano i costi.

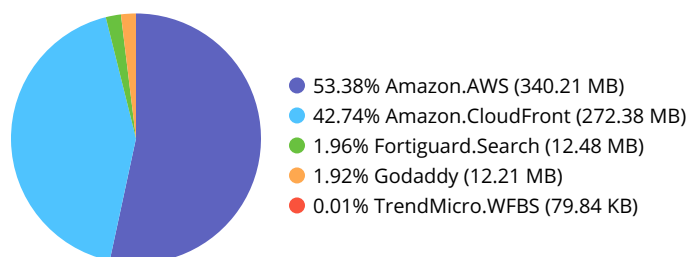
### Uso del cloud (SaaS)



I responsabili IT sono spesso inconsapevoli di quanti servizi cloud sono in esecuzione nel proprio ambiente. Queste applicazioni possono essere talvolta utilizzate per eludere o persino sostituire risorse aziendali già disponibili per gli utenti in nome della facilità di impiego. Purtroppo però l'effetto collaterale è il possibile trasferimento di informazioni riservate al cloud e la conseguente potenziale esposizione dei dati, qualora l'infrastruttura di sicurezza del fornitore del cloud venga violata.

L'adozione di piattaforme IaaS (Infrastructure as a Service) è molto in voga e può risultare estremamente utile quando le risorse di elaborazione sono limitate o hanno speciali requisiti. Detto questo, l'efficace outsourcing dell'infrastruttura deve essere ben regolato per evitare abusi. La verifica occasionale delle applicazioni IaaS può essere un proficuo esercizio non solo a scopo di sicurezza, ma anche per finalità economiche, visto che può servire a ridurre al minimo i costi associati ai modelli pay-per-use o i canoni di abbonamento periodici.

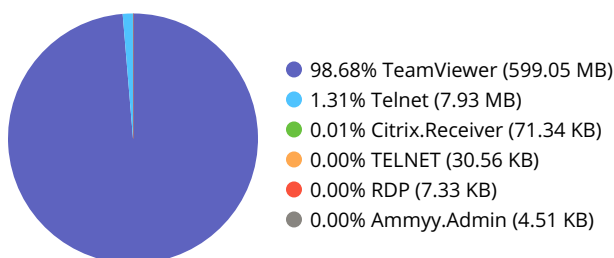
### Uso del cloud (IaaS)



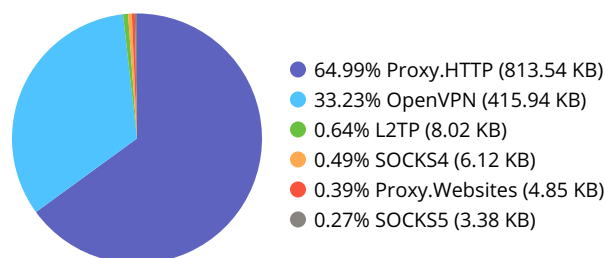
## Ulteriore scomposizione delle categorie di applicazioni

La definizione di sottocategorie di applicazioni può offrire informazioni preziose sull'efficienza con cui funziona la vostra rete aziendale. Alcuni tipi di applicazioni, come le P2P o quelle di gioco, non sono indispensabili all'ambiente aziendale e possono essere bloccate o limitate nella portata. Altre invece (come lo streaming di video/audio o i social media) hanno doppie finalità e possono essere gestite di conseguenza. Le tabelle seguenti illustrano le categorie di applicazioni ordinate in base alla larghezza di banda utilizzata durante il periodo di rilevamento.

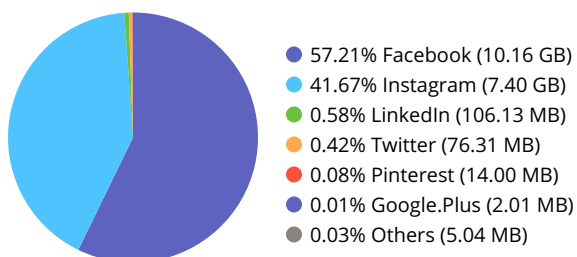
### Applicazioni di accesso remoto



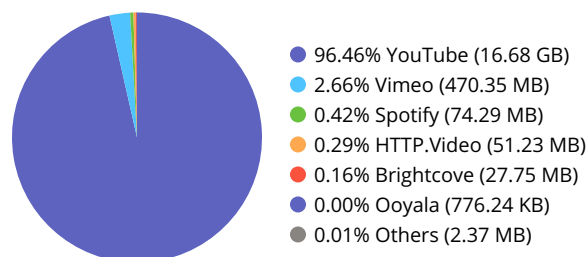
### Applicazioni proxy



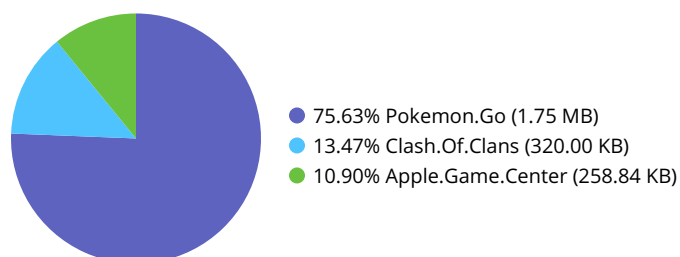
### Principali applicazioni social media



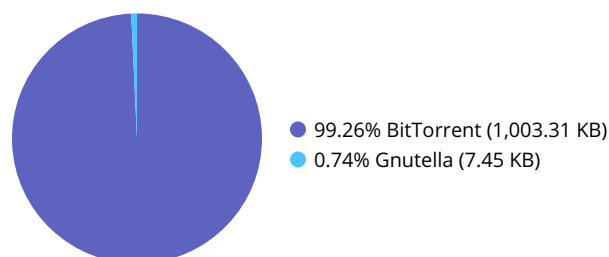
### Principali applicazioni di streaming video/audio



### Principali applicazioni di gioco













### Principali applicazioni Peer-to-Peer



## Uso del Web

Le abitudini di navigazione nel Web possono essere indicative di un impiego inefficiente delle risorse aziendali, ma anche di una scarsa ottimizzazione delle policy di Web Filtering. Possono inoltre fornire informazioni sui comportamenti di navigazione complessivi degli utenti aziendali e agevolare la definizione di linee guida per la conformità a norme e regolamenti d'impresa.

### Principali categorie Web

#	Categoria URL	Utenti	Numero	Larghezza di banda
1	 Information Technology	79	261,677	26.62 GB
2	 Advertising	60	191,639	3.27 GB
3	 Search Engines and Portals	71	122,870	4.77 GB
4	 Business	66	67,973	1.95 GB
5	 Social Networking	58	49,143	16.44 GB
6	 Content Servers	75	39,575	6.53 GB
7	 Meaningless Content	53	20,458	361.36 MB
8	 Streaming Media and Download	54	16,769	17.50 GB
9	 Government and Legal Organizations	64	14,921	1.83 GB
10	 News and Media	47	14,624	902.79 MB

Negli attuali ambienti di rete, molte più applicazioni di quanto ci si aspetti usano il protocollo HTTP per le comunicazioni. Il vantaggio principale di HTTP è che la comunicazione è ubiquitaria, universalmente accettata e (di norma) aperta su quasi tutti i firewall. Per la maggior parte delle applicazioni autorizzate e correlate al business, queste caratteristiche sono di beneficio, ma ci sono applicazioni non di tipo aziendale che utilizzano HTTP anche in modo poco produttivo e potenzialmente pericoloso.









### Principali applicazioni Web

#	Applicazione	Sessioni	Larghezza di banda
1	HTTPS.BROWSER	446,469	18.97 GB
2	YouTube	19,534	16.68 GB
3	MS.Windows.Update	3,131	10.49 GB
4	Facebook	38,740	10.16 GB
5	Instagram	10,853	7.40 GB
6	HTTP.BROWSER	68,214	4.53 GB
7	Google.Services	66,341	4.51 GB
8	Apple.Software.Update	18	1.85 GB
9	Microsoft.Office.Update	235	1.56 GB
10	HTTP.Segmented.Download	545	1.31 GB

## Siti Web frequentati











I siti Web visitati sono validi indicatori del modo in cui i dipendenti utilizzano le risorse aziendali e di come le applicazioni comunicano con specifici spazi Web. L'analisi dei domini a cui si è avuto accesso può condurre a modifiche dell'infrastruttura aziendale mirate, ad esempio, a bloccare determinati siti Web, eseguire accurate ispezioni delle app cloud e implementare tecnologie di accelerazione del traffico Web.

### Domini Web più visitati

#	Dominio	Categoria	Visite
1	www.google-analytics.com	 Search Engines and Portals	11,576
2	update.eset.com	 Information Technology	11,565
3	dt.adsafeprotected.com	 Advertising	11,217
4	pagead2.google syndication.com	 Advertising	10,707
5	edf.eset.com	 Information Technology	10,117
6	www.acquistinretepa.it	 Business	9,039
7	www.google.com	 Search Engines and Portals	8,787
8	nqs-nl5-c14.youboranqs01.com	 Meaningless Content	8,305
9	www.google.it	 Search Engines and Portals	8,086
10	7.au.download.windowsupdate.com	 Information Technology	7,933

La stima dei tempi di navigazione per singoli siti Web può essere utile quando si prova a ottenere un quadro preciso dei siti Web più noti. I valori si riferiscono in genere a risorse Web interne come Intranet, ma possono indicare talvolta anche comportamenti eccessivi. I tempi di navigazione possono servire a giustificare l'implementazione di tecnologie di web caching o contribuire a definire policy d'uso aziendali.

### Principali siti Web per tempo di navigazione

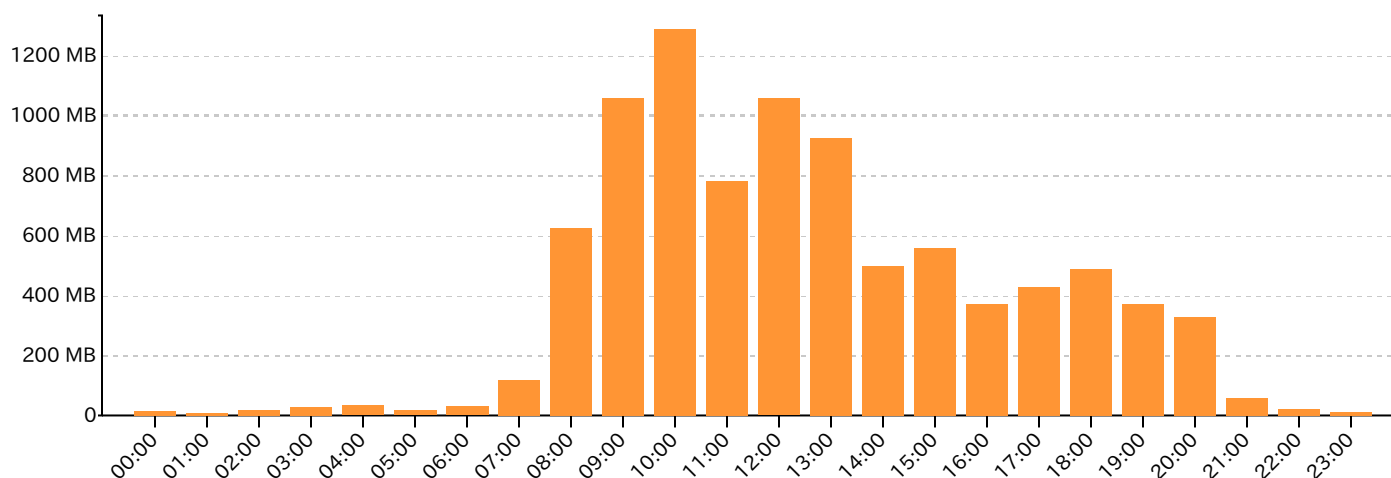
#	Siti	Categoria	Tempo di navigazione (hh:mm:ss)
1	www.google.com	 Business, Search Engines and Portals	68:21:26
2	safebrowsing.googleapis.com	 Information Technology, Search Engines and Portals	58:44:14
3	array603-prod.do.dsp.mp.microsoft.com	 Information Technology	58:22:18
4	graph.facebook.com	 Social Networking	58:05:59
5	www.google.it	 Business, Education, Entertainment, General Organizations, Government and Legal Organizations, Health and Wellness, Information Technology, Internet Radio and TV, News and Media, Newsgroups and Message Boards, Pornography, Reference, Search Engines and Portals, Society and Lifestyles	55:38:25
6	edge-mqtt.facebook.com	 Social Networking	55:00:15
7	adservice.google.it	 Search Engines and Portals	52:30:11
8	www.google-analytics.com	 Search Engines and Portals	48:10:05
9	settings-win.data.microsoft.com	 Information Technology	47:47:14
10	clients4.google.com	 Search Engines and Portals	46:04:52

# Utilizzo delle Rete

## Larghezza di banda

Esaminando l'uso della larghezza di banda nell'arco di un giorno medio, gli amministratori possono comprendere meglio i requisiti di velocità di interfacce e connessioni ISP dell'organizzazione. La larghezza di banda può anche essere ottimizzata applicazione per applicazione (con l'impiego della limitazione), definendo priorità tra gli utenti nelle ore di massimo traffico e ripianificando gli aggiornamenti al di fuori dell'orario di lavoro.

### Larghezza di banda media per ora



Tra i modi più efficaci di analizzare la larghezza di banda c'è quello di osservare le destinazioni e le origini che generano maggior traffico. I siti di destinazione più visitati (ad es. i siti Web esterni), come quelli per gli aggiornamenti di sistemi operativi e firmware, possono essere sottoposti a limitazioni per agevolare il traffico prioritario essenziale per il business. Gli host con elevato traffico possono poi essere ottimizzati internamente con l'ausilio del traffic shaping o di policy d'uso aziendali.

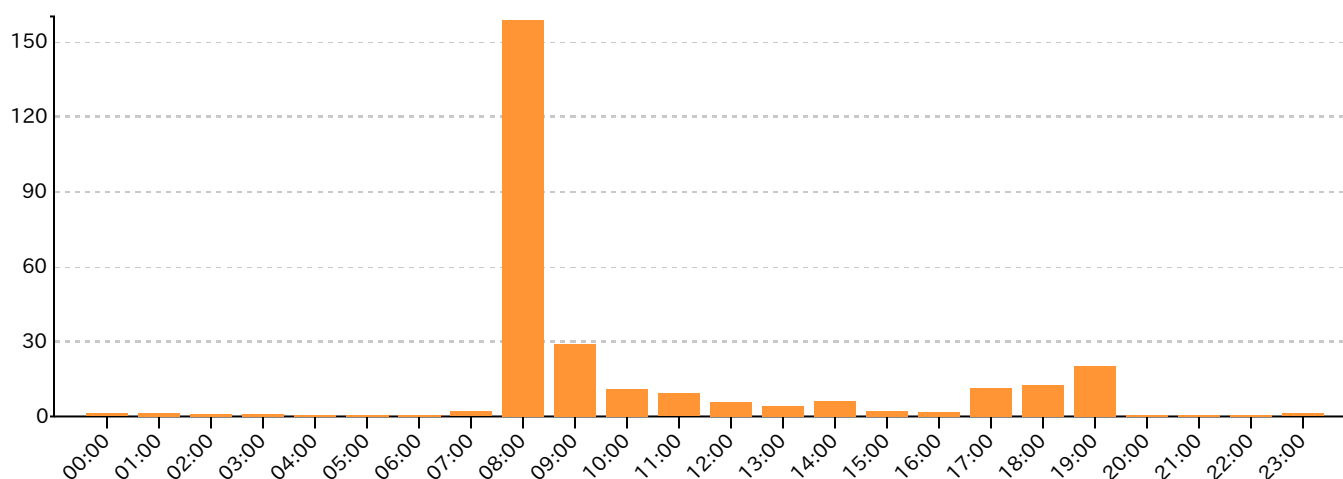
### Principali origini/destinazioni avide di larghezza di banda

#	Nome host	Larghezza di banda
1	scontent-mxp1-1.cdninstagram.com	6.38 GB
2	video-mxp1-1.xx.fbcdn.net	4.39 GB
3	test.eolo.it:8080	3.87 GB
4	7.au.download.windowsupdate.com	3.11 GB
5	scontent-mxp1-1.xx.fbcdn.net	2.69 GB
6	videodemand-vh.akamaihd.net	2.51 GB
7	7.tlu.dl.delivery.mp.microsoft.com	2.30 GB
8	vod08.msfn.cdnet.net	2.09 GB
9	officecdn.microsoft.com.edgesuite.net	1.55 GB
10	3.tlu.dl.delivery.mp.microsoft.com	1.55 GB

## Informazioni di dimensionamento

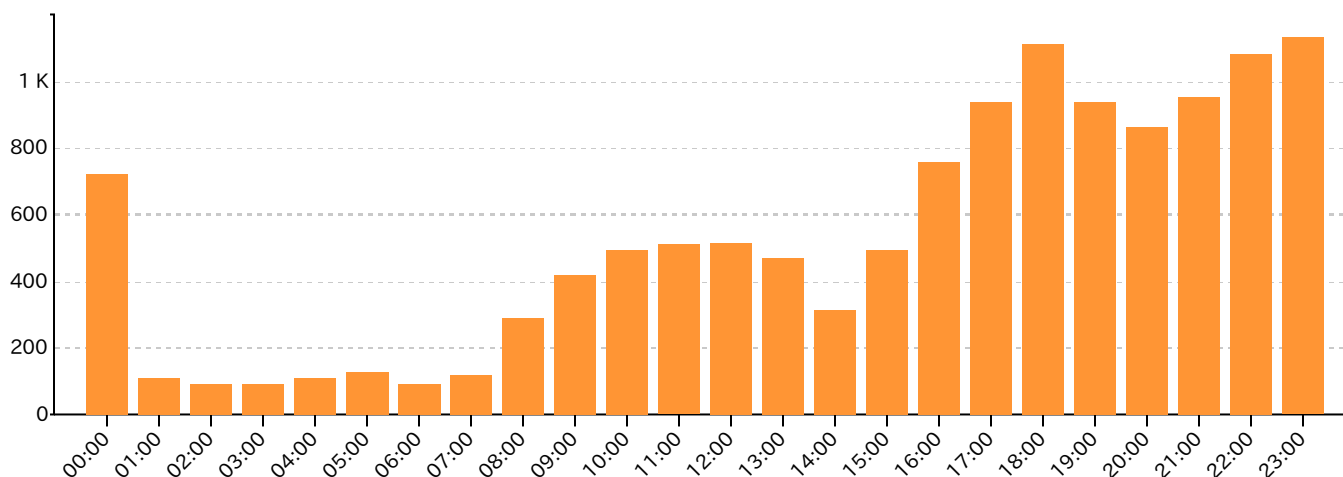
Conoscere gli intervalli di registrazione medi è estremamente utile per dimensionare un ambiente di sicurezza in un'ottica incentrata sulle performance. Valori più alti in determinate ore indicano in genere traffico di picco e throughput. Calcolare gli intervalli di registrazione per l'intera impresa può anche servire a dimensionare l'ambiente per l'impiego di dispositivi di registrazione/analisi a monte, come FortiAnalyzer. È importante notare che gli intervalli di registrazione qui illustrati sono stati calcolati con tutte le funzionalità di registrazione del FortiGate attivate e includono ogni tipo di log (traffico, antivirus, applicazioni, IPS, Web ed eventi di sistema).

### Intervallo di registrazione medio per ora



Il numero medio di sessioni richiamate nell'arco di un'ora può essere indicativo di requisiti prestazionali (non solo per FortiAnalyzer, ma anche per la soluzione FortiGate progettata finale). Esiste, in genere, una correlazione tra throughput, intervalli di registrazione e numero di sessioni. Le sessioni sono un altro parametro utilizzabile non solo per capire come dimensionare la rete corrente ma anche per saggiare il funzionamento della rete in presenza di maggiori velocità di traffico.

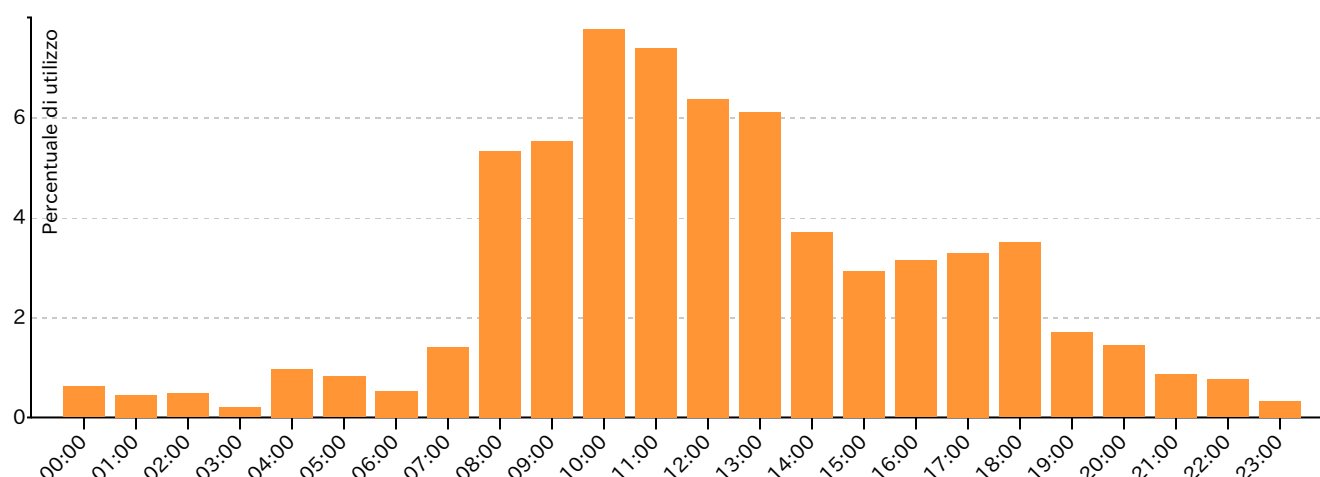
### Numero medio di sessioni per ora



## Statistiche relative al firewall

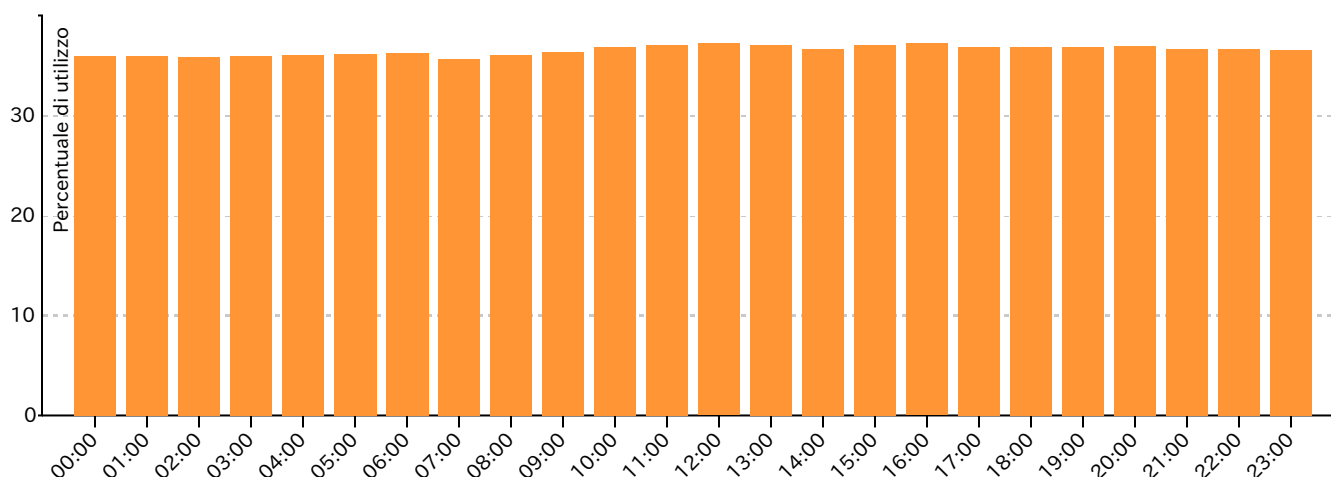
Il rilevamento dell'uso della CPU da parte di un FortiGate viene spesso utilizzato per realizzare una soluzione finale delle dimensioni corrette. Esaminando una suddivisione oraria dei dati statistici sull'impiego della CPU, è facile farsi un'idea realistica di come i FortiGate funzioneranno nella rete target. In genere più alto è il throughput maggiori saranno i log generati. Nel caso di un utilizzo prolungato del 75% o superiore, per l'implementazione finale potrebbero essere richiesti un modello più potente o un'architettura modificata.

### Utilizzo medio della CPU di FortiGate per ora



Analogamente, l'uso della memoria è un segnale della sostenibilità del FortiGate nella rete di destinazione. Questo valore può restare alto anche quando il throughput è relativamente basso, a causa dell'attività di registrazione (o di registrazione in coda) nel tempo.

### Utilizzo medio della memoria di FortiGate per ora



## Sicurezza e servizi FortiGuard

Per garantire una sicurezza efficace occorre conoscere il panorama delle minacce e saper rispondere rapidamente ai pericoli a più livelli. Sono centinaia i ricercatori di FortiGuard Labs impegnati ogni giorno in analisi mirate a scoprire nuove minacce e sviluppare contromisure efficaci per proteggere ogni azienda nel mondo. Queste persone sono il motivo per cui a FortiGuard è stata attribuito il merito di aver individuato oltre 250 attacchi zero-day e vulnerabilità e per cui le soluzioni di sicurezza Fortinet si aggiudicano punteggi così alti nei test di efficacia in condizioni reali di NSS Labs, Virus Bulletin, AV Comparatives e molti altri.



### **Funzioni di Application Control e IPS di nuova generazione**

L'Application Control e l'Intrusion Prevention (IPS) sono tecnologie di sicurezza essenziali per i firewall di nuova concezione come FortiGate. Imprese in tutto il mondo utilizzano l'Application Control e l'IPS della piattaforma FortiGate per gestire le proprie applicazioni e bloccare le intrusioni in rete (ogni minuto di ogni singolo giorno FortiGuard blocca circa 470.000 tentativi di intrusione). L'efficacia delle funzioni di Application Control e IPS dei FortiGate è comprovata dagli appositi test comparativi di settore di NSS Labs, che collocano continuamente le nostre soluzioni nei posti più alti in classifica.



### **Web Filtering**

Ogni minuto di ogni singolo giorno, FortiGuard Labs elabora circa 43 milioni di richieste di categorizzazione degli URL e blocca 160.000 siti Web malevoli. Il servizio di Web Filtering valuta più di 250 milioni di siti e genera quasi 1,5 milioni di classificazioni di nuovi URL ogni settimana. FortiGuard è l'unica soluzione di Web Filtering ad aver ottenuto la certificazione VBWeb essendo riuscita a bloccare il 97,7% dei download diretti di malware nei test del 2016.



### **AntiVirus e Mobile Security**

Ogni minuto di ogni singolo giorno, FortiGuard Labs neutralizza circa 95.000 programmi malware che prendono di mira piattaforme tradizionali, mobili e IoT. Tecnologie brevettate consentono a FortiGuard AntiVirus di identificare migliaia di varianti malware presenti e future con una sola signature, ottimizzando l'efficacia e le performance della sicurezza. Fortinet ottiene costantemente eccellenti risultati nei test di efficacia di Virus Bulletin e AV Comparatives.



### **AntiSpam**

Ogni minuto di ogni singolo giorno, FortiGuard Labs blocca circa 21.000 messaggi email di spam e, ogni settimana, produce quasi 46 milioni di regole antispam nuove e aggiornate. L'email è il primo vettore di attacco avanzato a carico delle organizzazioni e una strategia di sicurezza incisiva non può pertanto fare a meno di un potente antispam.







### **Advanced Threat Protection (FortiSandbox)**

Migliaia di aziende in tutto il globo utilizzano FortiSandbox per identificare minacce avanzate. FortiSandbox riceve costantemente il titolo di applicazione consigliata per i sistemi di rilevamento delle violazioni da NSS Labs nei test di settore e, nei test NSS Labs del 2015, ha ottenuto un punteggio superiore al 97%.



### **IP Reputation**





Ogni minuto di ogni singolo giorno, FortiGuard Labs blocca circa 32.000 tentativi di Command&Control di botnet. Tra i momenti critici della sequenza di attacco contro un'organizzazione c'è quello in cui la minaccia comunica con il server di Command&Control, per scaricare altre minacce o esfiltrare i dati sottratti. La funzione di reputation degli indirizzi IP e di dominio blocca questa comunicazione, neutralizzando le minacce.

 		Tipo documento: <b>Relazione Tecnica</b>		
 				
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>				
Emesso da:	<b>B.S/C.PSD</b>		Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

# Relazione Tecnica

## per la fornitura di “Servizi di Cloud Computing” SPC CLOUD LOTTO1

### Comune di Monte di Procida

 		Tipo documento: <b>Relazione Tecnica</b>	
 			
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

<b>REDATTO da:</b> (Autore)	<b>Citel Group</b>	<b>Antonio Leo</b>
<b>APPROVATO da:</b> (Proprietario)		<b>Citel Group</b>
<b>LISTA DI DISTRIBUZIONE:</b>		<b>Comune di Monte di Procida</b>





## REGISTRAZIONE MODIFICHE DOCUMENTO

La tabella seguente riporta la registrazione delle modifiche apportate al documento.

DESCRIZIONE MODIFICA	REVISIONE	DATA
Prima emissione	1	18/07/2018
Seconda emissione	1.1	20/09/2018

## Sommario

<b>REGISTRAZIONE MODIFICHE DOCUMENTO</b> .....	<b>2</b>
<b>1 SCOPO DEL DOCUMENTO</b> .....	<b>3</b>
<b>2 ANALISI</b> .....	<b>4</b>
2.1 Note procedurali e riferimenti .....	4
2.2 Sicurezza perimetrale e analisi del traffico .....	6
2.2.1 Descrizione del contesto .....	6
2.2.2 Considerazioni preliminari .....	7
2.2.3 Analisi delle minacce .....	7
2.3 Analisi delle vulnerabilità.....	16
2.3.1 Analisi delle vulnerabilità sito web .....	17
2.3.2 Analisi delle vulnerabilità presenti sulla rete .....	22
<b>3 Conclusioni</b> .....	<b>24</b>
3.1.1 Non Conformità normative .....	25
3.2 Interventi Tecnologici.....	26

 		Tipo documento: <b>Relazione Tecnica</b>	
 			
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

## 1 SCOPO DEL DOCUMENTO

Il presente documento ha lo scopo di presentare i risultati relativi alle analisi condotte relativamente allo status quo della postura di sicurezza dell'ente.





L'indagine è stata svolta mediante l'impiego di sonde che hanno rilevato e analizzato:

- La sicurezza perimetrale
- La tipologia di traffico generato dall'Ente
- L'inventario degli assett informatici presenti sulla rete
- Le vulnerabilità presenti sulla rete
- La vulnerabilità del sito internet

I report generati dagli strumenti impiegati nelle analisi condotte fino alla data del 20/09/2018 sono allegati al presente documento in particolare:

1. Allegato 1 Report Fortinet relativo alla sicurezza perimetrale, nome file: Cyber Threat Assessment (it)-2018-07-24-0356
2. Report vulnerabilità Qualys:
  - 2.1. Sito web
    - 2.1.1.WAS\_monte\_20092018
    - 2.1.2.WAS\_monte\_08092018
    - 2.1.3.WAS\_monte\_03082018
  - 2.2. Scansione\_Vulnerabilità\_LAN
3. Inventario delle risorse presenti sulla LAN: Assett\_Inventory

Gli allegati saranno forniti in formato elettronico.

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

## 2 ANALISI

Nei prossimi paragrafi vengono esposti i risultati delle prime analisi condotte relativamente a:

- Sicurezza perimetrale
- Vulnerabilità
- Sicurezza della rete

### 2.1 Note procedurali e riferimenti

Le analisi sul traffico, più in generale sulla sicurezza perimetrale, e sulle vulnerabilità è stata effettuata impiegando sonde prodotte da due vendor in particolare:

- Fortinet per la sicurezza perimetrale
- Qualys per l'analisi delle vulnerabilità

La scelta di un Vendor come Fortinet è stata guidata dalle seguenti motivazioni:

- Fortinet è tra i primi tre vendor di sicurezza informatica a mondo, come indicato da Gartner<sup>1</sup>







Figura 1: Gartner giugno 2017

- I report di NSS Labs<sup>2</sup> hanno assegnato un rating "Recommended" per 4 anni consecutivi Fortinet in relazione alle caratteristiche di Next Generation Firewall e Security Value MAP

<sup>1</sup> Gartner Inc. è una società per azioni multinazionale leader mondiale nella consulenza strategica, ricerca e analisi nel campo dell'Information Technology con oltre 60.000 clienti nel mondo. L'attività principale consiste nel supportare le decisioni di investimento dei suoi clienti attraverso ricerca, consulenza, benchmarking, eventi e notizie è una società indipendente <https://www.gartner.com/technology/home.jsp>

<sup>2</sup> NSS LABS è la più grande organizzazione indipendente specializzata nell'analisi delle minacce informatiche. <https://www.nsslabs.com/company/about-nss/>

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>		Versione: <b>1.1</b> Data di emissione: <b>21/09/2018</b>

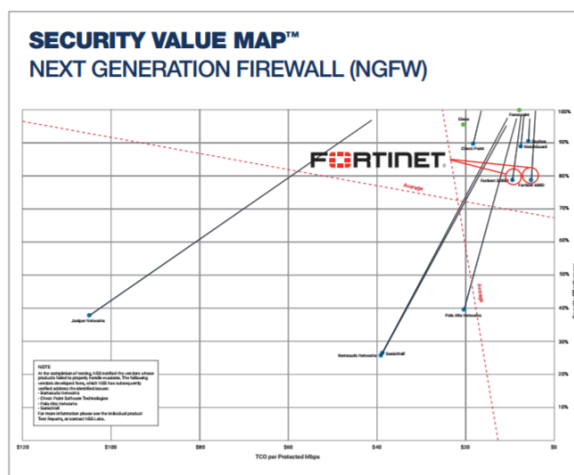


Figura 2: NSS LAB security value map 2017

- I report ICSA<sup>3</sup> dal 2016 al 2017, Fortinet Advanced Threat Protection (including FortiGate, FortiMail, FortiClient, and FortiSandbox) hanno superato gli standard “ICSA Advanced Threat Defense Standard (Network) and Email Certification”

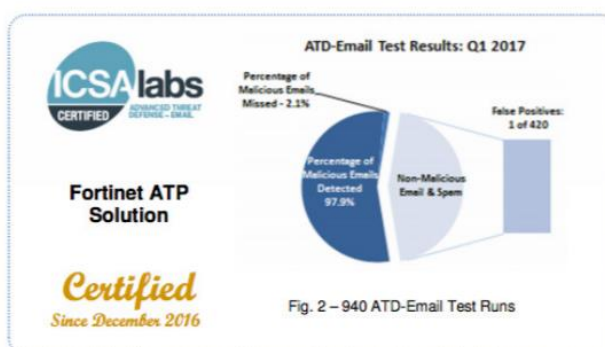
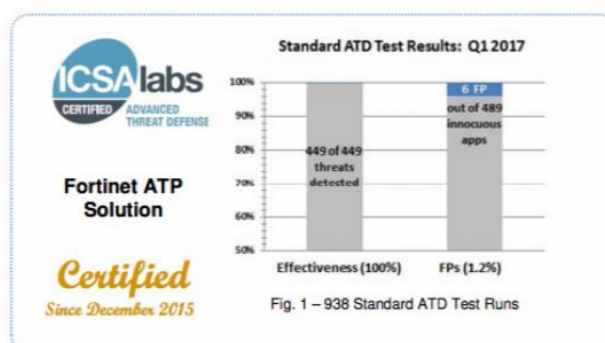






Figura 3: ICSA LABS 2017: Certificazione Advanced Threat Prevention

Le misurazioni riportate nei prossimi paragrafi, ed in particolare le numeriche di riferimento del settore e delle organizzazioni (intese come aziende) fanno riferimento alla knowledge base dell’installato Fortinet a livello mondo.

<sup>3</sup> ICSA LAB è una divisione indipendente di Verizon, tra le più autorevoli ed accreditate del settore, che dal 1989 si occupa di verificare, testare prodotti di sicurezza e IT. <https://www.icsalabs.com/about-icsa-labs>

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

Le analisi sono state effettuate relativamente al protocollo di comunicazione, non è stata effettuata alcuna operazione di spaccettamento dei dati o analisi del tipo di dato che è transitato sulla sonda.

Al fine di tutelare le informazioni riservate non sono stati tracciati gli IP delle macchine/host che hanno generato il traffico.

## 2.2 Sicurezza perimetrale e analisi del traffico

### 2.2.1 Descrizione del contesto

L'attuale infrastruttura di sicurezza è gestita da una macchina Cisco in end of support e con un numero limitato di licenze installate, che consente la protezione di 10 postazioni client. Il firewall in esercizio gestisce un collegamento vpn per il collegamento remoto alla infrastruttura di rete e alle risorse informatiche.

La rete gestisce 66 assett comprendenti postazioni di lavoro, stampanti, e telefoni voip, sulla base dell'ultimo assett inventory disponibile presso l'amministrazione.

La rete presenta una configurazione piatta, ovvero server, workstation, telefoni voip sono installati tutti sulla stessa rete.





Tutte le postazioni di lavoro sono configurate con IP assegnato manualmente e tutte sulla stessa subnet, non tutte le postazioni sono coperte dal firewall.

Esiste un dominio su un windows server 2003 e tutte le macchine collegate in rete hanno un'utenza dedicata, non vi sono policy che regolino l'utilizzo dello stesso.

Su tutte le macchine sono installati antivirus di tipo free, non è disponibile una gestione centralizzata, gli aggiornamenti sono effettuati manualmente quando si effettua un intervento di manutenzione su una postazione di lavoro (indicata nel seguito anche come end point)

I backup dei dati sono effettuati 2 volte al giorno su HDD USB collegati al server, in un secondo momento gli stessi vengono copiati manualmente su un NAS installato presso la sala server, non è stato possibile rilevare la presenza di una procedura o di un regolamento interno che disciplini le policy di back up e le procedure di disaster recovery.

La rete non presenta segmentazioni e sullo switch core è agganciata una seconda connettività dedicata alla navigazione per la biblioteca. Sono stati, inoltre, rilevati due 2 Access Point Wi-Fi privi di chiave di protezione.

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

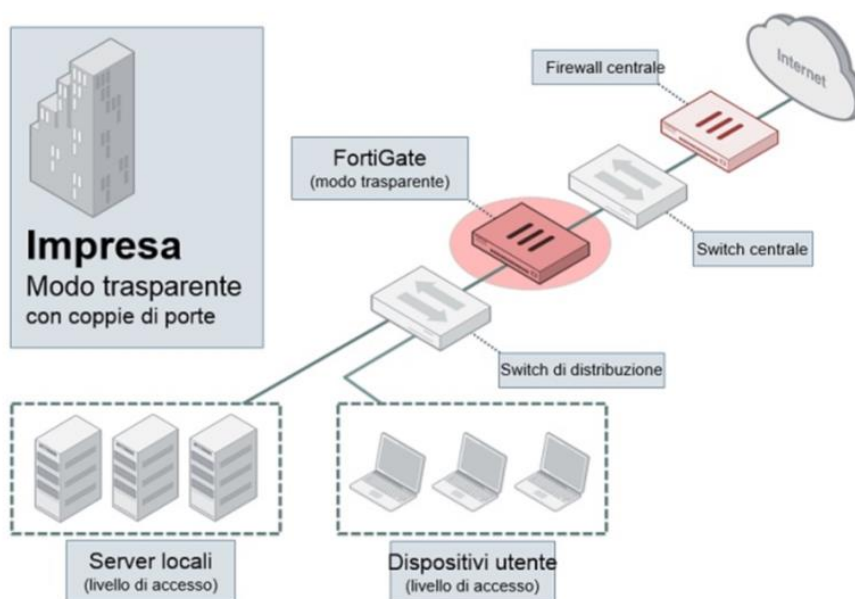
### 2.2.2 Considerazioni preliminari

1. Le caratteristiche funzionali degli apparati di sicurezza perimetrale attualmente in esercizio non consentono di rispondere all'attuale scenario di minacce informatiche
  - 1.1. I firmware e del sistema operativo non possono essere aggiornati in quanto non sono state sottoscritte le fee di manutenzione del Vendor
  - 1.2. Questa situazione comporta un elevato livello di rischio dal momento che sono presenti vulnerabilità note che non possono essere corrette.
2. Non sono presenti funzionalità di IPS, quindi si ha un elevato rischio di eventi avversi di sicurezza informatica
3. L'assenza di Content Filtering, AntiBot e del controllo del traffico cifrato (HTTPS) aumenta i rischi informatici legati alla navigazione Internet
4. Non sono disponibili strumenti di reportistica che consentano di identificare l'indirizzo IP interno o l'utenza che ha generato un tipo di traffico o ha subito attacco informatico.
5. L'assenza di un Antivirus a gestione centralizzata, non permette la realizzazione di una policy di sicurezza uniforme e non garantisce uno standard di protezione unico per gli end point, aumentando i rischi di incidente informatico.
6. La configurazione piatta della rete, senza segmentazione tra postazioni di lavoro, workstation e apparati voip, comporta elevati rischi di sicurezza in quanto, per esempio, una infezione su una workstation può raggiungere velocemente i server.

### 2.2.3 Analisi delle minacce

In data 11/07/2018 è stata installata una macchina Fortinet 100-e con le licenze UTM attive e collegata all'analyzer Fortinet, la sonda ha effettuato il monitoraggio per 15 gironi.

La macchina è stata installata davanti allo switch core e dietro i firewall in esercizio, in tal modo è stato possibile analizzare tutto il traffico che dalla rete interna andava verso internet e tutto il traffico proveniente dal mondo esterno dopo essere stato filtrato dalla infrastruttura di sicurezza in esercizio.





Titolo documento: **Assessment Tecnologico Monte di Procida**Emesso da: **B.S/C.PSD**Versione: **1.1**Data di emissione:  
**21/09/2018****Figura 4: posizione della sonda**

La sonda ha analizzato:

- Traffico in entrata sulla rete dopo il passaggio attraverso il firewall
- Traffico dalla rete verso il firewall

Di seguito si riportano i dati di misurazione sintetici:

TIPOLOGIA	Rilevazione	Rilevazione
Sicurezza e prevenzione delle minacce	Attacchi IPS	117.806
Sicurezza e prevenzione delle minacce	Malware/botnet	0
Sicurezza e prevenzione delle minacce	Siti Web malevoli rilevati	17
Produttività utenti	Applicazioni rilevate	238 di cui 13 ad elevato rischio
	Principale applicazione utilizzata	HTTPS. Browser
	Principale categoria applicativa	Web.Client
	Siti Web visitati: Principale sito Web	11822 update.eset.com
Utilizzo della rete	Larghezza di banda totale	97.07 GB
	Host con il numero di sessioni più elevato:	192.168.50.248
	Intervallo di registrazione medio/sec.	12.37
	Host principale per larghezza di banda	192.168.50.248

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

L'Amministrazione subisce quotidianamente 117.806 attacchi IPS, gli attacchi IPS cercano di sfruttare le vulnerabilità applicative per by-passare l'infrastruttura di sicurezza e permettono agli aggressori di introdursi nell'organizzazione.

#	Gravità	Nome minaccia	Tipo	Vittime	Fonte	Numero
1	5	<a href="#">Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution</a>	Code Injection	1	1	266
2	5	<a href="#">Apache.Struts.2.REST.Plugin.Remote.Code.Execution</a>	Code Injection	1	1	168
3	5	<a href="#">Cisco.IOS.HTTP.Command.Execution</a>	Improper Authentication	1	1	42
4	5	<a href="#">Necurs.Botnet</a>		1	1	28
5	5	<a href="#">Bash.Function.Definitions.Remote.Code.Execution</a>	OS Command Injection	1	1	24
6	5	<a href="#">Adobe.Coldfusion.BlazeDS.Java.Object.Deserialization</a>	Code Injection	1	1	14
7	5	<a href="#">Apache.Commons.Collection.InvokerTransformer.Code.Execution</a>	OS Command Injection	1	1	14
8	5	<a href="#">Accellion.FTA.Cookie.Information.Disclosure</a>	Information Disclosure	1	1	14
9	5	<a href="#">MS.IIS.WebHits.Authentication.Bypass</a>	Improper Authentication	1	1	14
10	5	<a href="#">SWEEditServlet.DirectoryTraversal</a>	Path Traversal	1	1	14

Figura 5: principali vulnerabilità rilevate

La presenza di queste vulnerabilità mette in evidenza:

1. il rischio di esfiltrazione di dati
2. il rischio di perdere il controllo degli host della rete
3. l'assenza di una policy di patching management

In base ai dati disponibili, ed in considerazione della mancanza di strumenti IPS si può affermare che l'organizzazione è esposta ad un elevato rischio di data breach o evento avverso di sicurezza informatica.

Dall'analisi della tipologia del traffico emerge che il traffico generato dall'organizzazione è principalmente di tipo HTTPS.

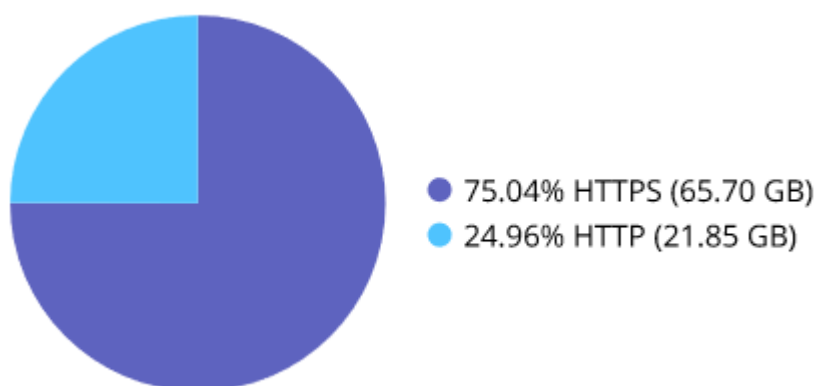






Figura 6: traffico http e https

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

L'uso del traffico HTTPS presenta un rischio specifico legato al fatto che, mancando gli strumenti, non è possibile ispezionare il contenuto dei pacchetti in transito sul WEB, emerge il rischio di esfiltrazione di dati non autorizzati. Al fine di ridurre i rischi legati al traffico HTTPS emerge l'esigenza di dotarsi di strumenti che consentano di gestire l'analisi del traffico HTTPS.

La sonda ha rilevato l'uso di applicazioni IaaS/SaaS. La Figura 7 riporta le prime 10 applicazioni per livello di rischio utilizzate dalla organizzazione:





- le applicazioni di categoria proxy potrebbero essere utilizzate (generalmente in maniera intenzionale) per bypassare le misure di sicurezza applicate. Può accadere, ad esempio, che gli utenti aggirino il firewall camuffando o criptando le comunicazioni esterne. In molti casi, questo può essere considerato un atto doloso e una vera e propria violazione delle policy d'uso aziendali.
- le applicazioni di accesso remoto sono impiegate per accedere ad host interni, aggirando così il sistema NAT o tracciando un percorso di accesso secondario (backdoor) agli host interni. Nei casi peggiori, l'accesso remoto può servire a favorire l'esfiltrazione dei dati e l'uso improprio delle risorse aziendali.
- Sono inoltre presenti applicazioni Peer to Peer che possono essere usate per bypassare i controlli dei contenuti ed eseguire trasferimenti di dati non autorizzati o in violazione del diritto di autore.

#	Rischio	Nome applicazione	Categoria	Tecnologia	Utenti	Larghezza di banda	Sessioni
1	5	Proxy.HTTP	Proxy	Network-Protocol	2	813.54 KB	176
2	5	SOCKS4	Proxy	Network-Protocol	1	6.12 KB	36
3	5	SOCKS5	Proxy	Network-Protocol	1	3.38 KB	18
4	5	Proxy.Websites	Proxy	Browser-Based	2	4.85 KB	3
5	4	Telnet	Remote.Access	Client-Server	822	7.96 MB	7,116
6	4	BitTorrent	P2P	Peer-to-Peer	2	1,003.31 KB	1,320
7	4	TeamViewer	Remote.Access	Client-Server	9	374.76 MB	1,238
8	4	Citrix.Receiver	Remote.Access	Client-Server	2	71.34 KB	200
9	4	RDP	Remote.Access	Client-Server	2	7.33 KB	37
10	4	Gnutella	P2P	Peer-to-Peer	1	7.45 KB	36

**Figura 7: le prime 10 applicazioni a più alto rischio**

In relazione a quanto sopra esposto la mancanza di strumenti e regolamenti interni che disciplinino l'uso di delle applicazioni espone il cliente a:

- Rischio di esfiltrazione di dati
- Violazione della normativa sulla privacy
- Violazione della normativa sui diritti di autore
- Uso improprio delle risorse aziendali

 		Tipo documento: <b>Relazione Tecnica</b>	
 			
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>








Di seguito si riportano gli host che sono stati valutati come a maggior rischio e che subiscono il maggior numero di attacchi.

#	Dispositivo	Punteggio
1	192.168.50.235	625,515
2	192.168.50.249	21,125
3	SERVIZISOCIALI	20,565
4	192.168.50.248	14,325
5	SCENIC	13,620
6	192.168.50.227	10,345
7	TRIBUTI	8,625
8	MONTEDIPROCIDA	5,000
9	COMANDO1	1,955
10	ARCHILLIANO	1,175





**Figura 8: indirizzi ed host maggiormente sotto attacco**

I dati sopra esposti mettono in evidenza la necessità di ricorrere ad una segmentazione della rete.

Di seguito si riportano i paesi di origine verso cui viene effettuata la maggiore navigazione e/o trasmissione di dati.

#	Paese	Larghezza di banda
1	 China	2.54 MB
2	 United States	1.04 MB
3	 Russian Federation	627.56 KB
4	 Vietnam	485.33 KB
5	 Korea, Republic of	368.47 KB
6	 Italy	283.64 KB
7	 Egypt	271.68 KB
8	 Turkey	271.62 KB
9	 Hong Kong	238.81 KB
10	 Sweden	220.53 KB

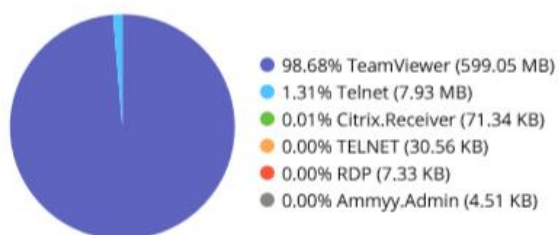
**Figura 9: paesi origine degli attacchi**

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

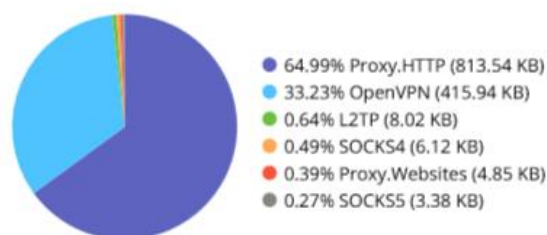
### 2.2.3.1 ANALISI DELLA PRODUTTIVITÀ E IMPIEGO DELLA BANDA

L'analisi ha consentito anche di valutare la produttività e l'utilizzo della banda internet.

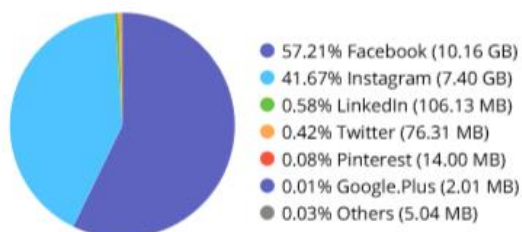
#### Applicazioni di accesso remoto



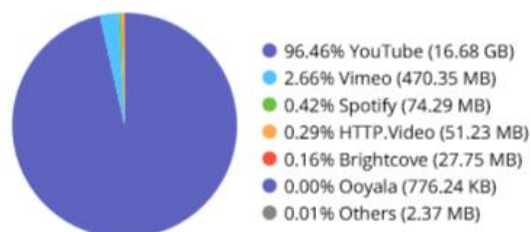
#### Applicazioni proxy



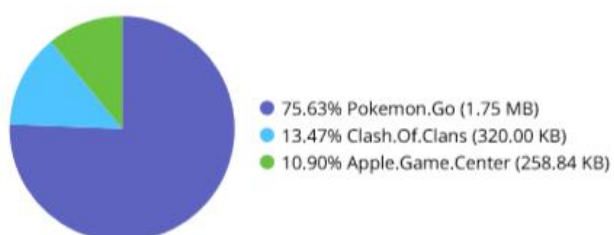
#### Principali applicazioni social media



#### Principali applicazioni di streaming video/audio



#### Principali applicazioni di gioco



#### Principali applicazioni Peer-to-Peer

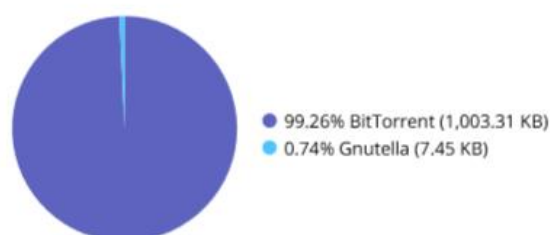
















Figura 10: utilizzo applicazioni della rete

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

La Figura 11 mostra le principali categorie di navigazione ed il relativo impiego di banda.

#	Categoria URL	Utenti	Numero	Larghezza di banda
1	 Information Technology	79	261,677	26.62 GB
2	 Advertising	60	191,639	3.27 GB
3	 Search Engines and Portals	71	122,870	4.77 GB
4	 Business	66	67,973	1.95 GB
5	 Social Networking	58	49,143	16.44 GB
6	 Content Servers	75	39,575	6.53 GB
7	 Meaningless Content	53	20,458	361.36 MB
8	 Streaming Media and Download	54	16,769	17.50 GB
9	 Government and Legal Organizations	64	14,921	1.83 GB
10	 News and Media	47	14,624	902.79 MB

**Figura 11: principali categorie di navigazione**

I dati sopra riportati consentono di valutare le abitudini di navigazione nel Web del personale e possono essere un utile strumento a supporto della definizione delle policy di navigazione e delle istruzioni da fornire ai dipendenti per l'impiego delle risorse aziendali.

A parte la presenza di importante navigazione verso i social media i dati mettono in evidenza un uso della rete in linea con il core business aziendale.





#	Applicazione	Sessioni	Larghezza di banda
1	HTTPS.BROWSER	446,469	18.97 GB
2	YouTube	19,534	16.68 GB
3	MS.Windows.Update	3,131	10.49 GB
4	Facebook	38,740	10.16 GB
5	Instagram	10,853	7.40 GB
6	HTTP.BROWSER	68,214	4.53 GB
7	Google.Services	66,341	4.51 GB
8	Apple.Software.Update	18	1.85 GB
9	Microsoft.Office.Update	235	1.56 GB
10	HTTP.Segmented.Download	545	1.31 GB

**Figura 12: impiego di banda per tipo di applicazioni**

La Figura 12 mette in evidenza come la banda viene utilizzata dagli utenti, evidenzia la necessità di:

- Dotarsi di uno strumento che consenta di analizzare il traffico criptato
- Un regolamento aziendale che definisca le policy di navigazione
- Uno strumento che consenta di applicare il regolamento, implementando policy differenziate per tipologia/categorie di utenti e tipo di applicazioni

Dall'analisi della navigazione è emersa la presenza di navigazione verso siti malevoli, per siti Web malevoli si intendono quegli spazi online che ospitano software/malware concepiti per raccogliere informazioni di

 		Tipo documento: <b>Relazione Tecnica</b>	
 			
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

nascosto, danneggiare il computer host o manipolare in altro modo la macchina bersaglio senza il consenso dell'utente. La sonda ha rilevato la navigazione verso 6 siti malevoli, è plausibile pensare che tale navigazione sia legata ad un incauto utilizzo delle risorse da parte degli utenti, ma è opportuno sottolineare che uno strumento di controllo della navigazione può ridurre o eliminare drasticamente gli accessi a questo tipo di website.

Inoltre è stata rilevata la navigazione verso siti di fishing, siti che emulano le pagine di siti Web leciti nel tentativo di raccogliere informazioni personali o riservate (login, password, ecc.) degli utenti finali.

Valutando l'impiego di applicazioni SaaS si può notare:

## Uso del cloud (SaaS)

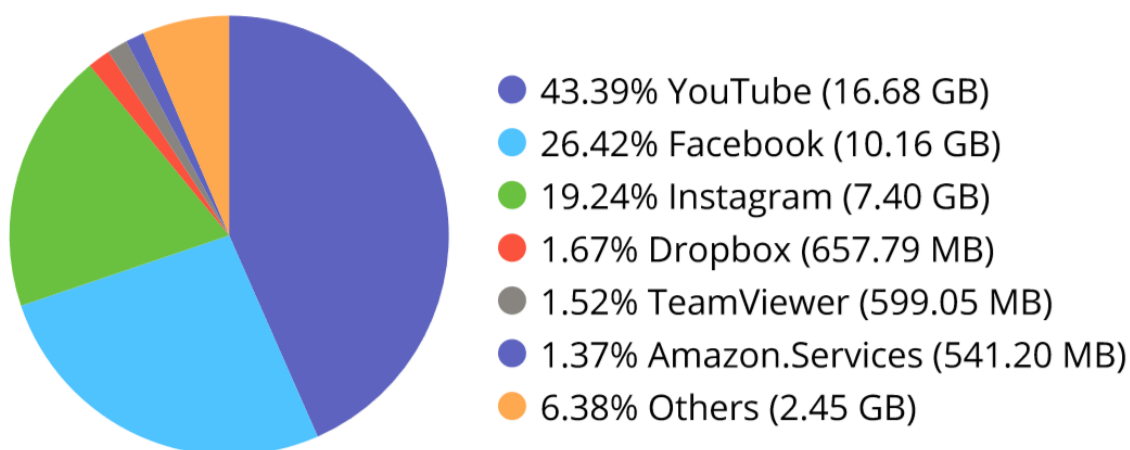



Figura 13: uso di piattaforme SaaS

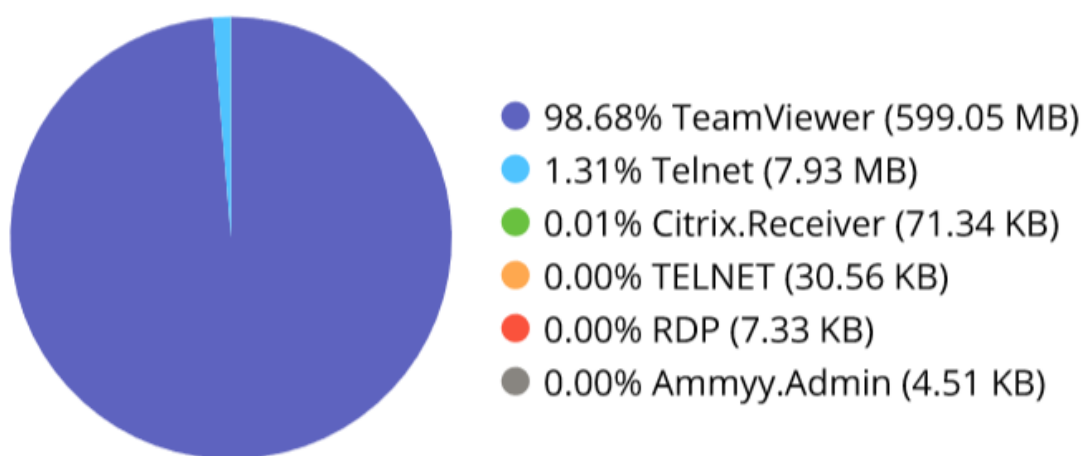
- Elevato traffico verso la piattaforma Youtube, l'accesso a questo tipo di servizio comporta:
  - Riduzione delle performance di banda
  - Un uso improprio delle risorse aziendali qualora non vi siano policy che disciplinino l'accesso a tali servizi
  - Anche in presenza di policy organizzative adeguate, l'attuale infrastruttura di sicurezza non ne consente la gestione ed il monitoraggio
- Elevato traffico dati su Dropbox, fenomeno di SHADOW IT, espone l'organizzazione ad elevato rischio di esfiltrazione di dati
  - L'uso di questo servizio soprattutto, se non disciplinato da policy organizzative, espone l'organizzazione ad elevati rischi di violazione della normativa sui dati personali in quanto non è possibile verificare che tipo di dati sono oggetto di condivisione

		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

- La mancanza di uno strumento che consenta di bloccare l'utilizzo evidenzia una forte carenza di sicurezza ed una responsabilità importante del Titolare e del Responsabile in materia di protezione dei dati
- Traffico importante verso le piattaforme Facebook ed Instagram:
  - Uso improprio delle risorse aziendali, qualora non vi siano regolamenti organizzativi interni che ne disciplinano l'utilizzo
  - Occupazione impropria della banda
  - Rischio di esfiltrazione di dati

Le rilevazioni relative alle altre piattaforme SaaS evidenziano il rischio di un uso improprio delle risorse aziendali soprattutto nel caso in cui non esista una policy organizzativa che ne disciplina l'impiego.





## Applicazioni di accesso remoto



**Figura 14: applicazioni proxy**

Queste applicazioni vengono utilizzate (generalmente in maniera intenzionale) per bypassare le misure di sicurezza applicate. Può accadere, ad esempio, che gli utenti aggirino il firewall camuffando o criptando le comunicazioni esterne. In molti casi, questo può essere considerato un atto doloso e una vera e propria violazione delle policy d'uso aziendali.

La mancanza di strumenti che consentano di disciplinare l'utilizzo di questo tipo di applicazioni comporta elevati rischi per la sicurezza dell'organizzazione dal momento che non è possibile non solo monitorare il tipo di traffico generato e ma anche la fonte origine del traffico stesso.

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

### 2.3 Analisi delle vulnerabilità

La scelta del Vendor Qualys è legata alla esigenza dettata dalla normativa di utilizzare un servizio Cloud per la gestione delle vulnerabilità.

L'analisi della vulnerabilità è effettuata sulla base di controlli approfonditi valutando la conformità agli standard SANS<sup>4</sup>, CIS<sup>5</sup> e OWASP<sup>6</sup>. Gli standard indicati rappresentano uno standard internazionale per misure e valutare la sicurezza di una infrastruttura IT, di una applicazione e di un software. Al fine di comprendere l'autorevolezza degli standard sopra indicati questi sono stati adottati da AGID come criteri di riferimento nella definizione delle misure minime di sicurezza per le pubbliche amministrazioni<sup>7</sup>.

Le vulnerabilità rilevate vengono classificate sulla base dei seguenti punteggi da 1 a 5 in ordine crescente per gravità:

Gravità	Descrizione
<b>1 Minimal</b>	Rilevazione di informazioni di base (es. tipo di web server, linguaggi di programmazione) che potrebbero facilitare l'individuazione di ulteriori vulnerabilità
<b>2 Medium</b>	Presenza di informazioni sensibili circa la piattaforma applicativa, come la versione del software in uso. Con queste informazioni un attaccante può sfruttare facilmente specifiche note vulnerabilità di una specifica versione del software. Altro tipo di informazioni sensibili possono essere scoperte in poche linee di codice o directory nascoste.
<b>3 Serious</b>	Queste vulnerabilità sono relative al non utilizzo di misure di sicurezza o exploit come per esempio trasmissione apertura del codice sorgente o la trasmissione di credenziali di autenticazione attraverso un canale non criptato.
<b>4 Critical</b>	Un attaccante può sfruttare queste vulnerabilità per guadagnare informazioni altamente sensibili contenute nell'applicazione o effettuare attacchi verso terzi usando cross-site Scripting o attacchi SQL.
<b>5 Urgent</b>	Un attaccante può sfruttare questo tipo di vulnerabilità per compromettere i dati dell'applicazione, ottenere informazioni circa gli account degli utenti eseguire comandi su un host in all'interno dell'applicazione

Le scansioni sono state realizzate mediante una sonda fisica installata presso il CED dell'amministrazione ed in particolare sulle classi di rete





- 192.168.50.1-192.168.50.234-254

<sup>4</sup><https://www.sans.org/critical-security-controls>

<sup>5</sup><https://www.cisecurity.org/>

<sup>6</sup>[https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)

<sup>7</sup>[http://www.agid.gov.it/sites/default/files/documentazione/misure\\_minime\\_di\\_sicurezza\\_v.1.0.pdf](http://www.agid.gov.it/sites/default/files/documentazione/misure_minime_di_sicurezza_v.1.0.pdf), pagina 4, pagina 6 della Direttiva

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

Mentre le vulnerabilità del sito internet sono state rilevate sulla mediante l'impiego di una sonda esterna Qualys.

### 2.3.1 Analisi delle vulnerabilità sito web

Il sito <https://www.montediprocida.gov.it/> stato sottoposto a scansione attraverso il sistema di rilevazione delle vulnerabilità Qualys, la scansione è stata effettuata nelle date del 09/08/2018, 03/09/2018 e 20/09/2018.

I report generati dalla scansione sono allegati alla presente relazione, e forniti in formato elettronico al referente di progetto: WAS\_monte\_20092018, WAS\_monte\_08092018, WAS\_monte\_03082018.

Di seguito si riportano dati sintetici relativi alle scansioni effettuate nei giorni:

Data Rilevazione		09/08/2018	03/09/2018	20/09/2018
Livello di rischio Generale		Alto	Alto	Alto
Numero di Vulnerabilità rilevate per severità	Severity 1	22	22	10
	Severity 2	155	155	18
	Severity 3	6	6	10
	Severity 4	0	0	2
	Severity 5	20	20	0

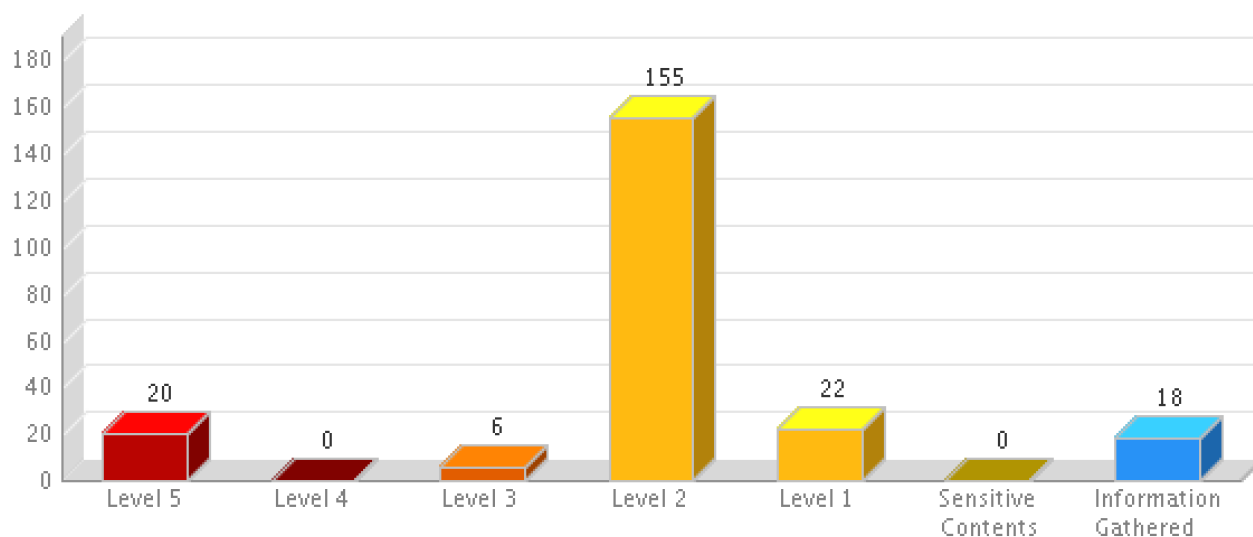


Figura 15: vulnerabilità al 09/08/2018

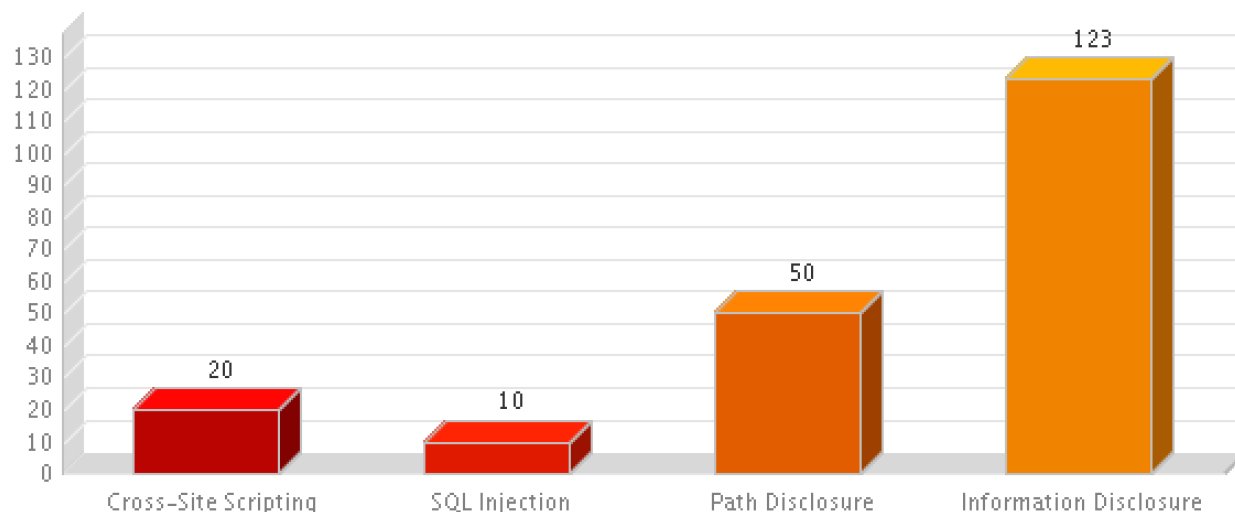
Titolo documento: **Assessment Tecnologico Monte di Procida**Emesso da: **B.S./C.PSD**Versione: **1.1**Data di emissione:  
**21/09/2018**

Figura 09/08/2018 Vulnerabilità per gruppi

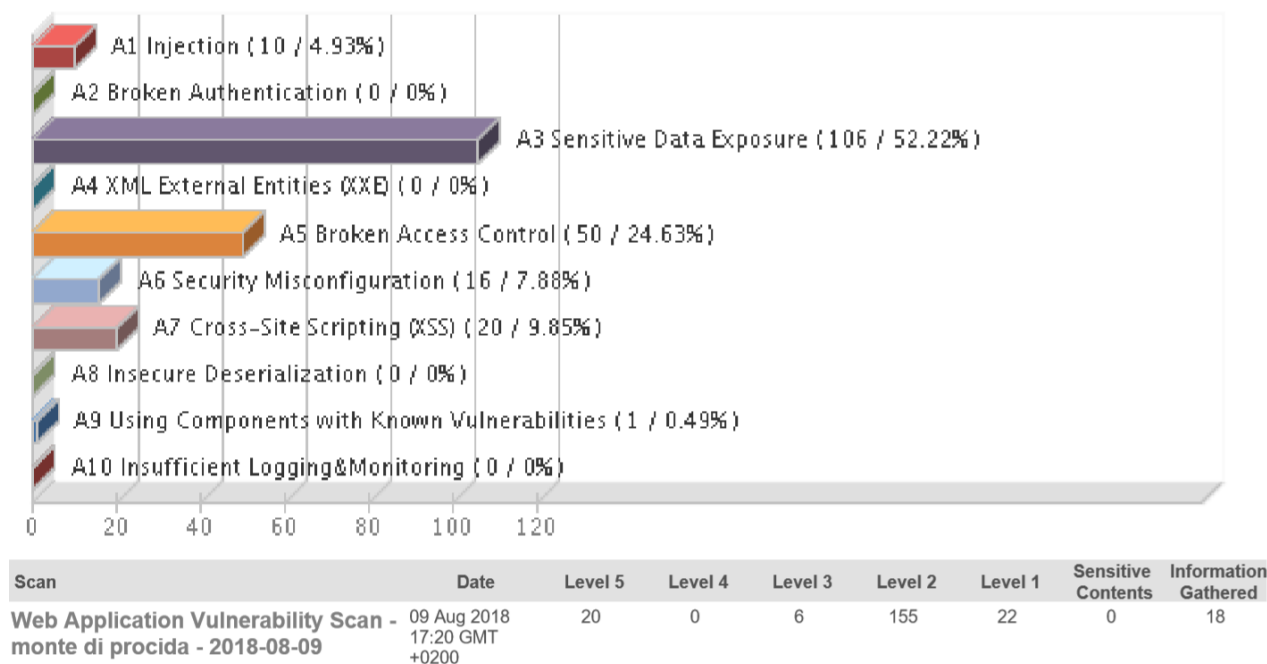


Figura 16: Vulnerabilità OSWAP 09/08/2018

Titolo documento: **Assessment Tecnologico Monte di Procida**

Emesso da: **B.S/C.PSD**

Versione: **1.1**

Data di emissione:  
**21/09/2018**

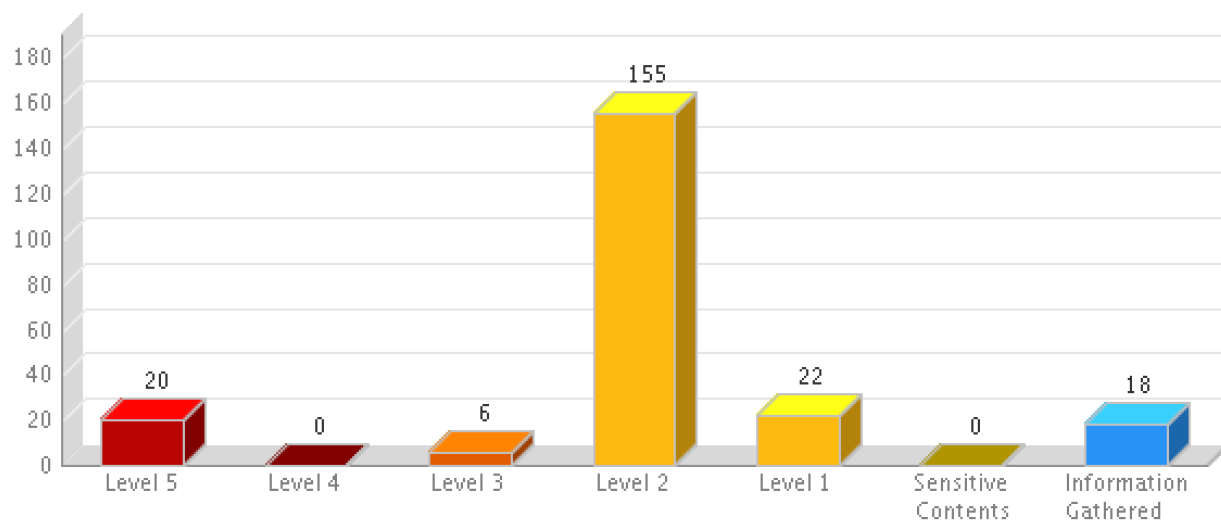


Figura 17:scansione del 03/09/2018

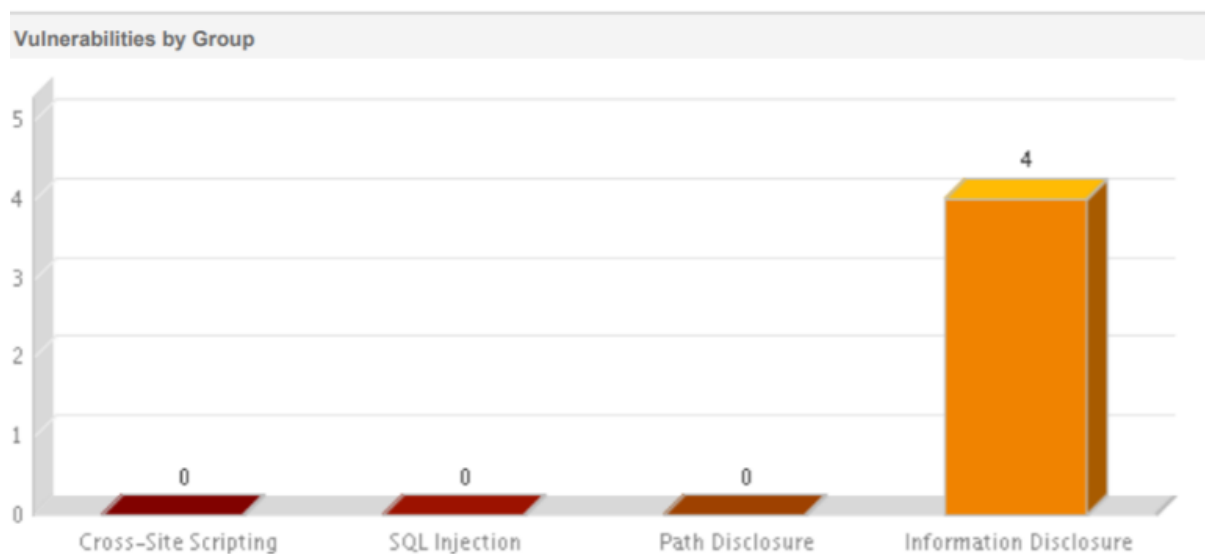


Figura 18: scansione del 03/09/2018

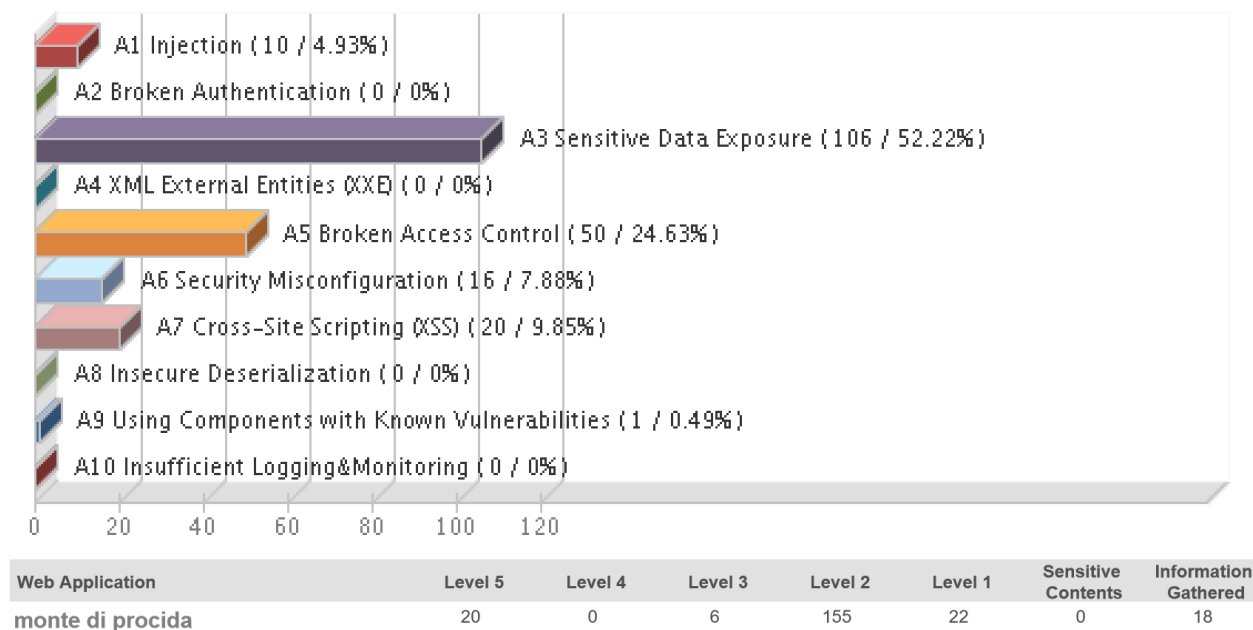
Titolo documento: **Assessment Tecnologico Monte di Procida**Emesso da: **B.S/C.PSD**Versione: **1.1**Data di emissione:  
**21/09/2018**

Figura 19: owasp 03/09/2018

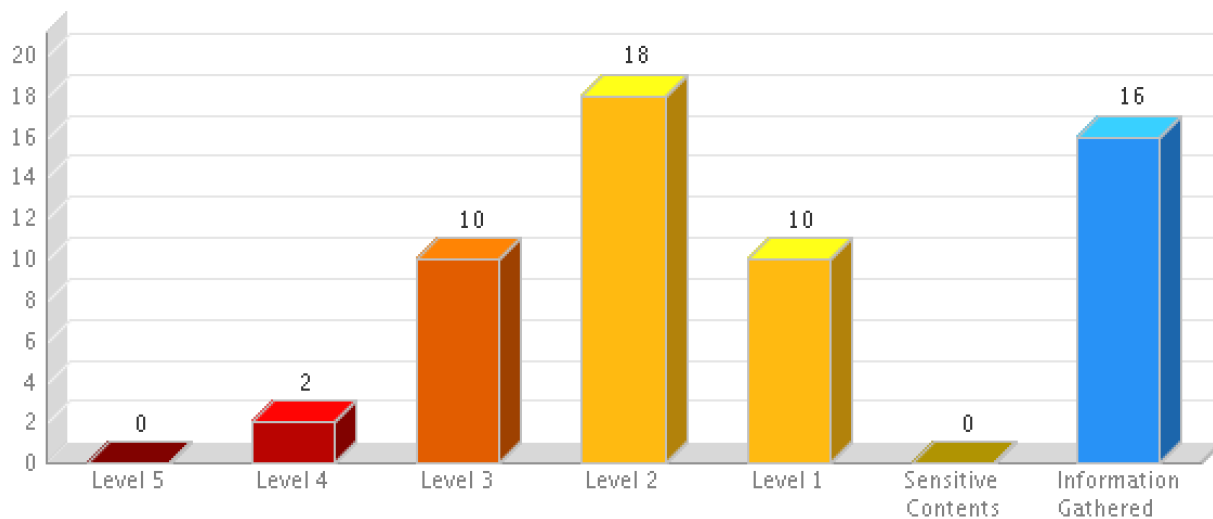


Figura 20: vulnerabilità al 20/09/2018

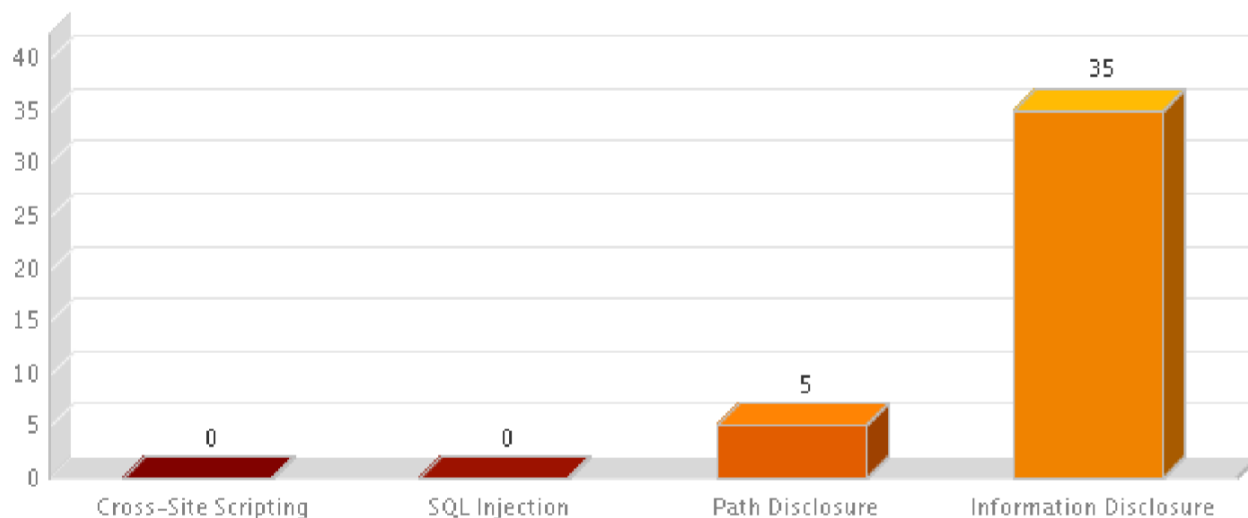
Titolo documento: **Assessment Tecnologico Monte di Procida**Emesso da: **B.S/C.PSD**Versione: **1.1**Data di emissione:  
**21/09/2018**

Figura 21:vulnerabilità per gruppo al 20/09/2018

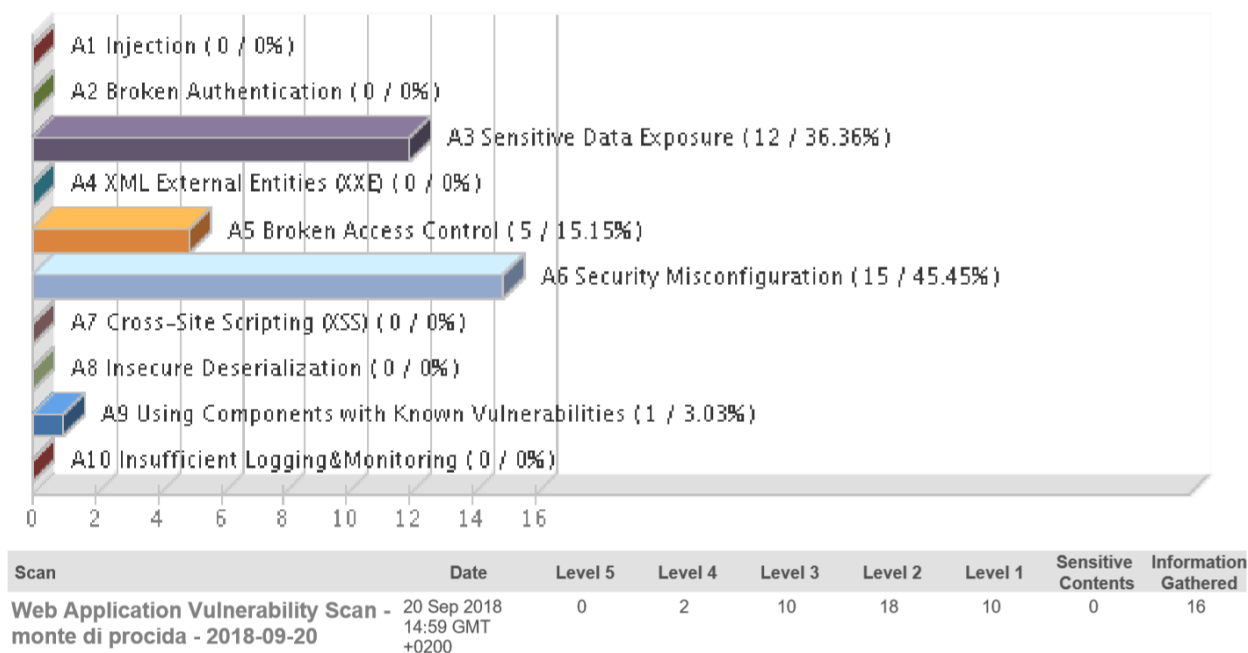






Figura 22: owasp al 20/09/2018

Le scansioni hanno messo in evidenza che:

- il livello di rischio del sito è ALTO
- viene effettuata un'attività di patching con cadenza temporale almeno bimestrale
  - il patching è relativamente efficace
- è necessario dotarsi di uno strumento che consenta di pianificare ed agire in maniera mirata sulle vulnerabilità

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

### 2.3.2 Analisi delle vulnerabilità presenti sulla rete

Utilizzando una sonda Qualys è stata analizzata la seguente classe di rete:192.168.50.1-192.168.50.234

Di seguito si riportano i dati di sintesi della scansione, per i dettagli si faccia riferimento all'allegato Scan\_Results\_ctegr5al2\_20180718\_scan\_1531903548\_30189.

In base a quanto esposto Figura 23: il livello di rischio degli asset è molto alto posizionandosi su un punteggio di 4,2 su una scala di 5.

Vulnerabilities Total		2365	Security Risk (Avg)		<div><div></div><div></div><div></div><div></div><div></div></div>	4.2
by Severity						
Severity	Confirmed	Potential	Information Gathered		Total	
5	48	16	0		64	
4	20	39	0		59	
3	150	101	104		355	
2	174	25	309		508	
1	24	3	1352		1379	
Total	416	184	1765		2365	

5 Biggest Categories					
Category	Confirmed	Potential	Information Gathered		Total
TCP/IP	26	0	487		513
Information gathering	13	2	396		411
General remote services	155	31	209		395
SMB / NETBIOS	78	6	186		270
Windows	47	59	58		164

Figura 23: Vulnerabilità Rilevate

Sono presenti vulnerabilità che espongono l'organizzazione a rischi di databreach elevati tenendo in considerazione l'infrastruttura di sicurezza in esercizio.

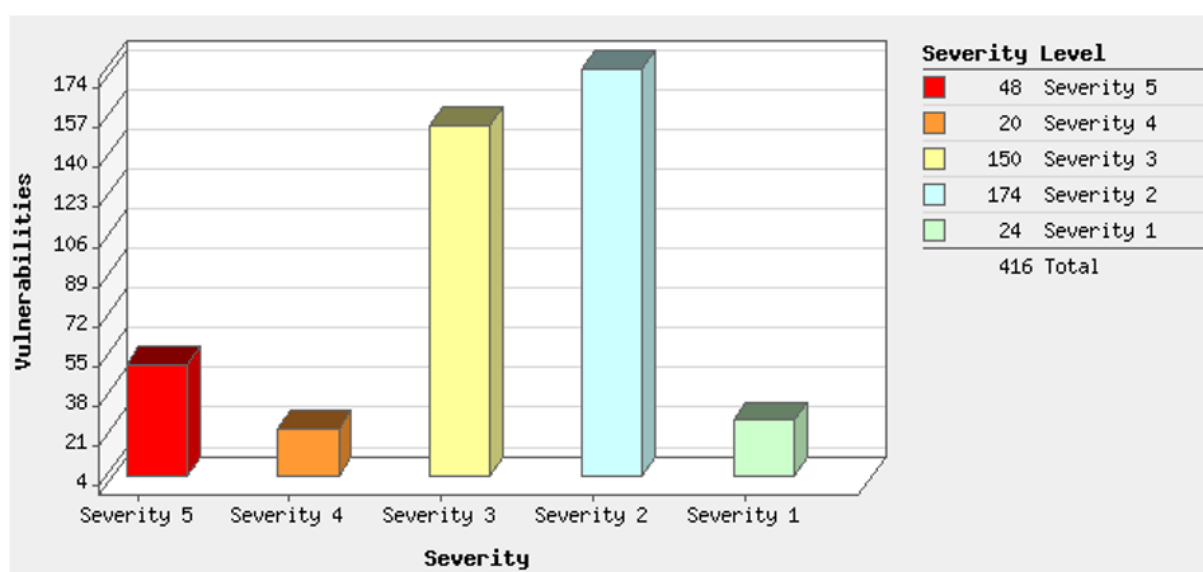


Figura 24: Vulnerabilità per gravità

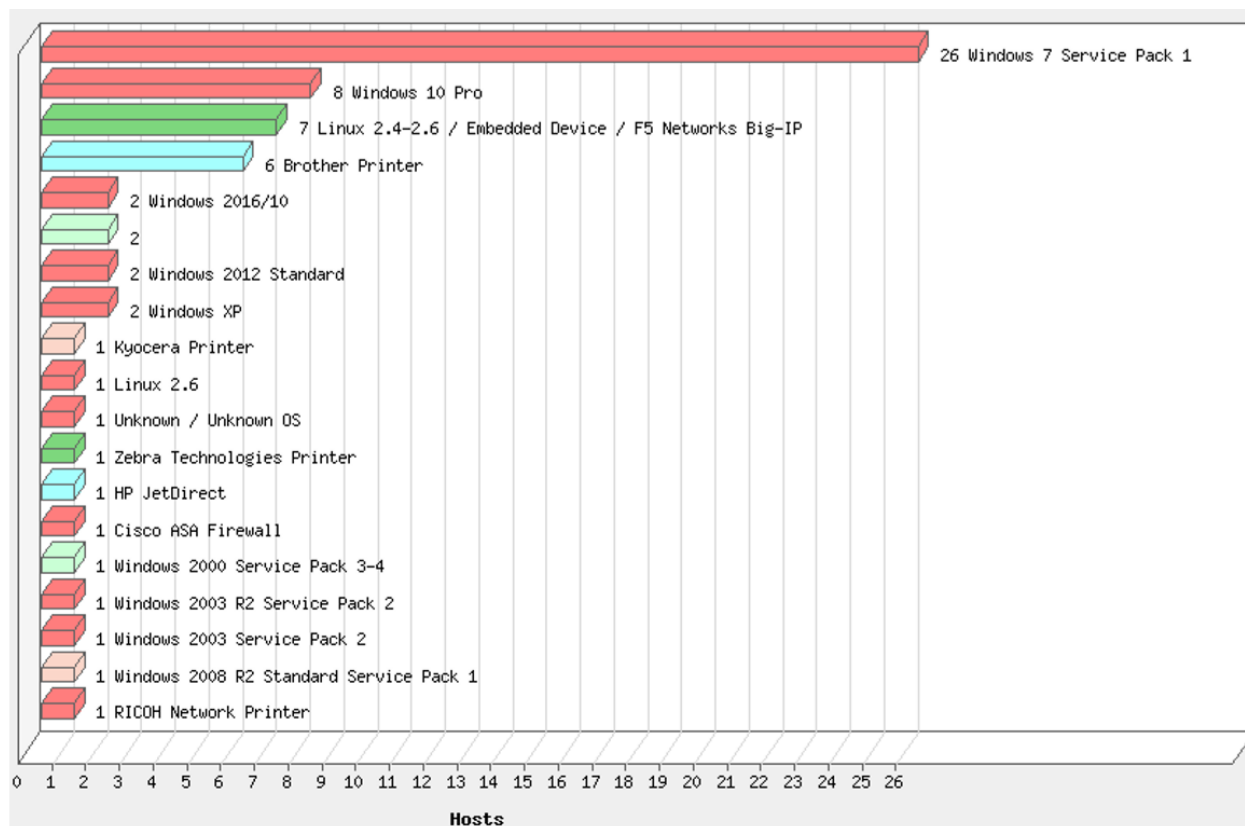
Titolo documento: **Assessment Tecnologico Monte di Procida**Emesso da: **B.S/C.PSD**Versione: **1.1**Data di emissione:  
**21/09/2018**





Figura 25: sistemi operativi rilevati

La scansione mette in evidenza un livello di rischio alto che potrebbe comportare:

- Presenza di macchine con sistemi operativi non più aggiornabili perché in end of support
- Presenza di vulnerabilità che potrebbero essere sfruttate per prendere il controllo dell'host al fine di:
  - Facilitare l'esfiltrazione di dati
  - Utilizzare le macchine come vettore di attacco
- Presenza di vulnerabilità che potrebbero essere sfruttate per
  - Raccogliere dati sensibili
  - Recuperare informazioni utili per ottenere dati sensibili o recuperare credenziali di accesso

La presenza di queste vulnerabilità oltre ad evidenziare un elevato livello di rischio evidenzia la necessità di realizzare una politica di patching management e dotarsi di uno strumento che consenta di monitorare e rilevare in maniera continuativa le vulnerabilità presenti sulla rete.

Il report completo della scansione sarà consegnato in formato elettronico.

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>





### 3 Conclusioni

La seguente tabella riporta una sintesi delle rilevazioni effettuate

Rilevazioni	Rischio
Attacchi alle vulnerabilità applicative	<ul style="list-style-type: none"> <li>• Esfiltrazione Dati</li> <li>• Controllo delle risorse</li> <li>• Elusione delle policy di sicurezza</li> </ul>
Navigazione verso siti Web malevoli rilevati	<ul style="list-style-type: none"> <li>• Furto di credenziali del personale</li> <li>• Esfiltrazione di dati</li> <li>• Esposizione ad attacchi</li> <li>• Mette in evidenza una scarsa sensibilità del personale verso la navigazione sicura</li> </ul>
Navigazione attiva verso siti Web di phishing	<ul style="list-style-type: none"> <li>• Furto di credenziali personali</li> <li>• Mette in evidenza una scarsa sensibilità del personale verso la navigazione sicura</li> </ul>
Applicazioni di accesso remoto rilevate	<ul style="list-style-type: none"> <li>• Esfiltrazione di dati</li> <li>• Bypass le policy di sicurezza</li> </ul>
Applicazioni P2P e di condivisione file	<ul style="list-style-type: none"> <li>• Esfiltrazione dati</li> <li>• Trasferimento e condivisione file in violazione di diritti di proprietà intellettuale</li> <li>• Informazioni sensibili</li> </ul>
Vulnerabilità applicative sito web	<ul style="list-style-type: none"> <li>• Esfiltrazione dati</li> <li>• Perdita controllo dell'host</li> </ul>
Vulnerabilità lan (parziale)	<ul style="list-style-type: none"> <li>• Presenza di vulnerabilità su due classi di rete che espongono al rischio di esfiltrazione di dati, perdita di controllo dell'host, esfiltrazione di credenziali di accesso</li> </ul>

È possibile affermare che:

- Le misure di sicurezza disponibili sono inadeguate allo scenario tecnologico attuale
- Esistono fenomeni di Shadow IT che non consentono di garantire una gestione sicura dei dati personali
- Visti i dati relativi alla navigazione verso siti malevoli e la presenza di infezioni veicolate tramite posta elettronica è necessaria la pianificazione di sessioni di formazione verso il personale al fine di sensibilizzare il personale all'utilizzo corretto ed informato sui rischi informatici
- Mancano strumenti che consentano di:

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

- Limitare l'uso improprio delle risorse aziendali
- Bloccare o limitare la navigazione Internet verso siti malevoli
- Individuare o ricostruire un databreach
- Garantire livelli di sicurezza adeguati alla tipologia di dati trattati dall'Amministrazione

Nei prossimi paragrafi si riporta la mappatura delle non conformità rispetto alle prescrizioni normative, in particolare la Circolare 18 aprile 2017, n. 2/2017 e il Regolamento Europeo 679/2016

### 3.1.1 Non Conformità normative

Rispetto a quanto previsto dal Regolamento Europeo in particolare in relazione all'obbligo di rilevazione e comunicazione in caso di data breach non è presente alcun strumento tecnico che consenta di:





- Rilevare un data breach
- Avviare la procedura di comunicazione al garante e agli interessati relativamente all'evento avverso

Descrizione	NORMA	STATO
Rilevazione data breach	art. 33 e 34 Regolamento UE 679/2016	NON CONFORME
Misure adeguate di sicurezza	art. 32 Regolamento UE 679/2016	NON CONFORME
Misure minime di sicurezza	Circolare 18 aprile 2017, n. 2/2017	NON CONFORME
Misure minime di sicurezza	Allegato B D.Lgs 196/2003	Parzialmente Conforme

In relazione alle misure minime di sicurezza risulta organizzate in base al livello di severità indicato dalla circolare AGID<sup>8</sup> risulta:

Livello di severità	NON CONFORME	PARZIALMENTE CONFORME	TBD	Totale c
A= "Alto": questi controlli possono riguardarsi come un obiettivo a cui tendere	27	4	1	32
M= "Minimo": i controlli in essa indicati debbono riguardarsi come obbligatori	35	9	1	45
S= "Standard": i controlli in essa indicati posso essere assunti come base di riferimento nella maggior parte dei casi	41	1	2	44
<b>Totale complessivo</b>	<b>103</b>	<b>14</b>	<b>4</b>	<b>121</b>

<sup>8</sup> Pag. 5 MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)

   		Tipo documento: <b>Relazione Tecnica</b>	
Titolo documento: <b>Assessment Tecnologico Monte di Procida</b>			
Emesso da:	<b>B.S/C.PSD</b>	Versione: <b>1.1</b>	Data di emissione: <b>21/09/2018</b>

Le righe in stato “TBD” devono essere oggetto di ulteriore verifica e/o possono essere corrette introducendo misure tecniche, procedurali organizzative.

Il dettaglio delle non conformità rilevate è disponibile in allegato “STATO AGID” alla presente relazione, che sarà fornito in formato elettronico.

Azioni correttive da adottare

Sulla base delle informazioni alla data scrivente e delle azioni finora intraprese risulta necessario valutare

### 3.2 Interventi Tecnologici

Lo stato dell’arte delle tecnologie in esercizio evidenzia:

1. per quanto esposto al capitolo 1.1.3 e 1.2 si un elevato livello di rischio di esfiltrazione dati dovuta all’inadeguatezza/manca di strumenti tecnologici
2. mancanza di strumenti tecnologici che consentano la rilevazione di un data breach
3. quasi completa non conformità alla Circolare 18 aprile 2017, n. 2/2017 che imponeva l’adeguamento al 31/12/2017

La seguente tabella indica sinteticamente i riferimenti normativi, lo stato di conformità e la relativa soluzione tecnica da adottare:

Descrizione	NORMA	STATO	SOLUZIONE TECNICA
Rilevazione data breach	art. 33 e 34 Regolamento UE 679/2016	<ul style="list-style-type: none"> <li>Alto Livello di rischio</li> <li>Nessuno Strumento</li> <li>Completa non conformità</li> </ul>	Sistema per la gestione e la correlazione degli eventi di sicurezza (SIEM) o in alternativa un sistema di gestione di analisi dei log
Misure adeguate di sicurezza	art. 32 Regolamento UE 679/2016	<ul style="list-style-type: none"> <li>Completa non conformità</li> <li>Dotazione tecnologica non adeguata e insufficiente</li> </ul>	<ul style="list-style-type: none"> <li>Sicurezza Perimetrale</li> <li>Sicurezza gateway navigazione</li> <li>Sistema sicurezza antibot</li> <li>Sistema di prevenzione esfiltrazione dati</li> </ul>
Misure minime di sicurezza	Circolare 18 aprile 2017, n. 2/2017-	<ul style="list-style-type: none"> <li>NON CONFORMITA’</li> </ul>	<ul style="list-style-type: none"> <li>Sicurezza dell’applicazioni</li> <li>Sistema Antivirus perimetrale</li> <li>Sicurezza della posta elettronica</li> <li>Sistema Antispam</li> <li>Sistema Antimalware</li> <li>Sistema Gestione Vulnerabilità</li> <li>Strumento per raccolta e analisi log di sicurezza perimetrale</li> <li>Sistema di protezione Zero Days</li> </ul>

# DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

Istituito ai sensi del D.Lgs. 30/06/2003 n. 196 Allegato B  
aggiornato al D.Lgs. 101/2018 (Regolamento Europeo 679/2016)

## INDICE

§.1 - SCOPO DEL DOCUMENTO	pag. 3
§.2 – CAMPO DI APPLICAZIONE	pag. 4
§.3 – LEGGI E NORME DI RIFERIMENTO	pag. 4
§.4 – DEFINIZIONI DI LEGGE E GLOSSARIO	pag. 6
§.5 – DATI GENERALI DELL’AZIENDA	pag. 21
§.6 – STRUTTURAZIONE DELL’AZIENDA	pag. 21
§.7 – DESCRIZIONE DEL CICLO LAVORATIVO	pag. 22
§.8 – TITOLARE DEL TRATTAMENTO	pag. 28
§.9 – RESPONSABILE DEL TRATTAMENTO	pag. 28
§.10 – RESPONSABILE DELLA PROTEZIONE DEI DATI	pag. 29
§.11 – ELENCO DEI TRATTAMENTI DEI DATI POSTI IN ESSERE DAL TITOLARE DEL TRATTAMENTO	pag. 30
§.12 – REGISTRI DEL TRATTAMENTO DEI DATI	pag. 34
§.13 – CARATTERISTICHE DELLE AREE E DEI LOCALI, NONCHE’ DEGLI STRUMENTI CON CUI SI EFFETTUANO I TRATTAMENTI	pag. 35

§.14 – ANALISI DEI RISCHI CHE INCOMBONO SUI DATI	pag. 37
§.15 – MISURE DA ADOTTARE PER GARANTIRE L’INTEGRITA’ E LA DISPONIBILITA’ DEI DATI	pag. 39
§.16 – CRITERI E MODALITA’ DI RIPRISTINO DEI DATI, IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO	pag. 40
§.17 – ANALISI DEL MANSIONARIO PRIVACY E DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI	pag. 41
§.18 – DESCRIZIONE DEI CRITERI DA ADOTTARE, PER GARANTIRE L’ADOZIONE DELLE MISURE MINIME DI SICUREZZA, IN CASO DI TRATTAMENTI DI DATI PERSONALI E SENSIBILI AFFIDATI ALL’ESTERNO	pag. 44
§.19 – CONTROLLO PERIODICO SULLO STATO DELLA SICUREZZA	pag. 45
§.20 – MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO	pag. 46

## **§.1 – SCOPO DEL DOCUMENTO**

Il Documento Programmatico sulla Sicurezza dei dati nel trattamento dei dati personali e sensibili, ha lo scopo di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali e sensibili effettuato dal Poliambulatorio in intestazione del presente Documento.

Il presente Documento Programmatico sulla Sicurezza dei dati (di seguito chiamato DPS) è stato redatto dal dott. Giuseppe Pugliese in qualità di Responsabile del Trattamento, che si è avvalso del dott. ing. Carlo Zuddas in qualità di consulente esterno.

Sono definiti tre aspetti fondamentali relativi alla sicurezza delle informazioni:

1. **Confidenzialità:** solo gli utenti autorizzati possono accedere alle informazioni necessarie.
2. **Integrità:** protezione contro alterazioni o danneggiamenti; tutela dell'accuratezza e completezza dei dati.
3. **Disponibilità:** le informazioni vengono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

Si considerano primari i due concetti di politica di sicurezza e di sistema di governo della sicurezza (di cui la prima costituisce uno degli aspetti) nonché dalla specificazione dei controlli di sicurezza (logici, fisici, procedurali) necessari per farla rispettare e del modo in cui questi devono essere realizzati, secondo un approccio simile a quello degli standard della serie ISO 9000 per la certificazione di qualità. I concetti di politica di qualità e di sistema di gestione della qualità sui quali tali serie si basa, sono sostituiti da quelli di politica di sicurezza dell'informazione e di sistema di governo della sicurezza dell'informazione o ISMS (Information Security Management System).

La politica di sicurezza è la specificazione ad alto livello degli obiettivi di sicurezza (espressi, come di consueto in termini di volontà di salvaguardare la riservatezza, l'integrità e la disponibilità dell'informazione in presenza di minacce) che l'organizzazione si propone di conseguire. L'ISMS, invece, è il complesso di procedure per il governo della sicurezza attuato e mantenuto dall'organizzazione per garantire nel tempo il soddisfacimento della politica di sicurezza.

## **§.2 – CAMPO DI APPLICAZIONE**

Il DPS, definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali e sensibili.

Il DPS riguarda tutti i seguenti dati:

- Personali,
- Sensibili
- Giudiziari.

Il DPS si applica al trattamento di tutti i dati personali e sensibili per mezzo di:

- Archivio cartaceo,
- Archivio Elettronico.

Il DPS deve essere conosciuto ed applicato da tutto il personale o collaboratori esterni del Poliambulatorio.

## **§.3 – LEGGI E NORME DI RIFERIMENTO**

Vengono di seguito riportati i principali testi legislativi in materia di sicurezza dei dati, e di cui si è tenuto conto per la stesura del presente DPS.

**D.Lgs. n. 255 del 28/07/1997** – Disposizioni integrative e correttive della legge 31 dicembre 1996, n. 675, in materia di notificazione dei trattamenti di dati personali, a norma dell'articolo 1, comma 1, lettera f), della legge 31 dicembre 1996, n. 676.

**D. Lgs. N. 171 del 13/05/1998** – Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica.

**D.Lgs. n. 389 del 06/11/1998** – Disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici.

**D.Lgs. n. 281 del 30/07/1999** – Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica.

**D.Lgs. n. 282 del 30/07/1999** – Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario.

**Regolamento Europeo 679/2016** – Regolamento generale sulla protezione dei dati.

**D.Lgs. n. 101 del 10/08/2018** – 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 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).

## **§.4 – DEFINIZIONI DI LEGGE E GLOSSARIO**

Si riportano alcuni trattamenti di dati in cui non è previsto il consenso:

- a) È necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- b) È necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- c) Riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
- d) Riguarda dati relativo allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- e) È necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'art. 82, comma 2;
- f) Con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397 (disposizioni in materia di indagini difensive), o comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

- g) Con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate e collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;
- h) Con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contratti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;
- i) È necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6 comma 2, del decreto legislativo 29 ottobre 1999 n. 490 (Testo unico delle disposizioni legislative in materia di beni culturali e ambientali), o secondo quanto previsto dai medesimi codici, presso altri archivi privati.

Si riportano di seguito alcune definizioni riportate nel Decreto Legislativo 30 giugno 2003 n. 196.

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti a raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Dato personale: qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato.

Dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati giudiziari: i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato.

Titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Comunicazione: il dar conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile.

Banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Garante: organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica. Tra i vari compiti del Garante si elencano i più importanti:

- controlla se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione,
- esamina i reclami e le segnalazioni e provvede ai ricorsi presentati dagli interessati o dalle associazioni,
- prescrive ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti,
- cura la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati.

Si riportano di seguito alcune definizioni riportate nel Decreto Legislativo 10 agosto 2018 n. 101.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione Europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Si riportano di seguito alcune definizioni riportate nel Regolamento Europeo 679/2016.

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificazione online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interesse specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione e degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione e degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Terzo: la persona fisica e giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento.

Impresa: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica.

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Obiezione pertinente e motivata: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza de rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione.

Altri termini riferiti all'impiego di strumentazione elettronica:

Comunicazione elettronica: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite un servizio di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate a un abbonato o utente ricevente, identificato o identificabile.

Chiamata: la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale.

Misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione: i dati e i dispositivi, in possesso di una persona, da questa conosciuti o a essa univocamente correlati, utilizzati per l'autenticazione informatica.

Parola chiave: componente di una credenziale di autenticazione associata a una persona e a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione: l'insieme delle informazioni, univocamente associate a una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti a essa consentiti.

Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

## GLOSSARIO

Accertamenti: il Garante può disporre accessi a banche dati, archivi o altre ispezioni e verifiche nei luoghi dove si svolge il trattamento o dove occorre effettuare rilevazioni utili al controllo del rispetto della normativa sulla privacy.

Accesso: l'interessato ha diritto a ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se ancora non registrati, e la loro comunicazione in forma intelligibile.

Autorizzazione: provvedimento adottato dal Garante con il quale il titolare (azienda, ente o libero professionista) viene autorizzato a trattare dati sensibili o giudiziari o a trasferire dati all'estero. Sette autorizzazioni generali adottate dall'Authority consentono trattamenti per scopi specifici, senza dover chiedere il singolo via libera.

Blocco: conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Cancellazione: diritto di ottenere l'eliminazione di dati per i quali è venuta meno la necessità di effettuare il trattamento. Non è possibile ottenere la distruzione o l'alterazione del documento se perdura l'obbligo legale di conservarlo.

Cessazione del trattamento: in caso di cessazione di un trattamento i dati possono essere distrutti, ceduti ad un altro titolare a condizione che siano destinati a un trattamento compatibile agli scopi per i quali sono raccolti. Possono essere conservati per fini personali e non usati per comunicazioni sistematiche o per la diffusione, oppure ceduti o tenuti per scopi storici, statistici o scientifici, rimanendo nell'ambito della legge, dei regolamenti, della normativa comunitaria e dei codici di deontologia e di buona condotta.

Codici di deontologia: il codice della privacy rafforza l'importanza dei codici di deontologia e di buona condotta, prevedendone la sottoscrizione in molteplici settori. Per alcuni, come quelli riferiti ai trattamenti delle “centrali rischi” private, delle attività investigative, per scopi statistici e di ricerca scientifica in ambito privato, i lavori sono in fase avanzata. In allegato al codice della privacy sono pubblicati quelli che dettano le linee guida ai trattamenti nel giornalismo, per scopi storici e per quelli statistici nell'ambito del sistema statistico nazionale.

Comunicazione: far conoscere dati personali a uno o più soggetti diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualsiasi forma, anche rendendoli disponibili o consultabili.

Consenso: qualsiasi trattamento di dati personali da parte di privati o di enti pubblici economici può essere effettuato solo con il consenso dichiarato dall'interessato, preventivamente informato da chi gestisce i dati. Il consenso deve essere manifestato liberamente e specificatamente in riferimento a un trattamento chiaramente individuato. Deve essere annotato dal titolare, dal responsabile o da un incaricato del trattamento su un registro o su un verbale. Può riguardare l'intero trattamento o una o più operazioni. Deve essere in forma scritta quando il trattamento riguarda i dati sensibili.

Controllo a distanza: il codice ribadisce il divieto di controllo a distanza dei lavoratori. In base allo statuto dei lavoratori impianti e apparecchiature di controllo richiesti da esigenze organizzative, produttive o di sicurezza sul lavoro dai quali derivi anche la possibilità di controllo dei lavoratori, possono essere installati solo previo accordo con le rappresentanze sindacali aziendali o, in mancanza, con la commissione interna. In difetto di accordo spetta all'Ispettorato Provinciale del Lavoro, su richiesta del datore, dettare le modalità di uso degli impianti di controllo.

Dati giudiziari: sono quei dati in grado di rivelare l'esistenza di provvedimenti giudiziari penali soggetti a iscrizione nel casello giudiziario (condanne definitive, libertà condizionale, divieto o obbligo di soggiorno, misure alternative alla detenzione). Rientrano fra questi anche la qualità di imputato o indagato.

Dati identificativi: sono i dati personali che consentono l'identificazione diretta dell'interessato.

Dati sensibili: si tratta di quei dati in grado di rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni o organizzazioni di carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare stato di salute e vita sessuale.

Dato anonimo: dato che in origine, o a seguito di trattamento, non può essere associato a un interesse identificato o identificabile.

Direttive Europee: il codice della privacy attua le direttive del Parlamento europeo e del Consiglio 95/46/CEE del 24 ottobre 1995 e 2002/58/CEE del 12 luglio 2002.

Discariche abusive: il controllo video di aree abusivamente impiegate come discariche di materiali e di sostanza pericolose è lecito se risultano inefficaci o inattuabili altre misure. Il medesimo controllo non è lecito se effettuato per accertare solo infrazioni amministrative rispetto a modalità e orari di deposito dei rifiuti urbani.

Elenchi di abbonati: il Garante individua insieme all'Autorità per le garanzie nelle comunicazioni le modalità di inserimento e utilizzo dei dati personali relativi agli abbonati negli elenchi cartacei o elettronici a disposizione del pubblico.

Fatturazione dettagliata: l'abbonato ha diritto a ricevere in dettaglio, a richiesta e senza aggravio di spesa, la dimostrazione degli elementi che compongono la fattura, relativi, in particolare, a data e ora di inizio della conversazione, numero selezionato e tipo di numerazione.

Garanti europei: organo consultivo europeo indipendente che si occupa di protezione dei dati personali.

Handicap: il codice della privacy ha introdotto una specifica norma relativa ai contrassegni rilasciati a persone invalide: devono essere esposti sui veicoli e contenere solo i dati indispensabili a individuare l'autorizzazione rilasciata, senza apposizione di simboli e diciture. Generalità e indirizzo della persona fisica interessata non devono essere direttamente visibili sul contrassegno.

Informativa: l'interessato è informato preventivamente, oralmente o per iscritto, su finalità e modalità di trattamento, natura obbligatoria o facoltativa del conferimento dei dati, conseguenze di un eventuale rifiuto a rispondere, soggetti e categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza, diritti, estremi identificativi del titolare e, se esistenti, del rappresentante nel territorio dello Stato e del responsabile. In caso di installazione di sistemi di videosorveglianza il cittadino deve essere informato sul fatto che sta per accedere in una zona videosorvegliata. L'informativa, in formato chiaramente visibile, deve indicare con formula sintetica la presenza di telecamere. Può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione.

Interpello preventivo: il ricorso al Garante può essere proposto solo dopo che è stata avanzata richiesta sul medesimo oggetto al titolare o al responsabile del trattamento, se sono decorsi i termini (15 giorni dal ricevimento senza riscontri, 30 giorni per un integrale riscontro alla richiesta) o si è ottenuto diniego, anche parziale.

Lavoro: nell'ambito lavorativo è vietato il controllo a distanza dei lavoratori, anche in caso di erogazione di servizi per via telematica mediante "web contact center". Sono previste particolari garanzie nei casi in cui le telecamere devono essere installate per esigenze organizzative e dei processi produttivi o sono richieste da esigenze legate alla sicurezza del lavoro. Inammissibili le telecamere in luoghi non destinati ad attività lavorativa come bagni, spogliatoi, docce, armadietti, e luoghi ricreativi.

Luoghi di cura: ammesso il monitoraggio dei pazienti ricoverati in particolari reparti, come, ad esempio, la rianimazione. Alle immagini possono accedere personale autorizzato e familiari dei ricoverati in reparti dove non sia consentito recarsi personalmente.

Minori: è vietato pubblicare e divulgare con qualsiasi mezzo notizie o immagini idonee a identificare minori, pure in caso di coinvolgimento del bambino in procedimenti giudiziari anche, non di natura penale.

Misure di sicurezza: i dati personali devono essere custoditi e controllati, al passo con lo sviluppo del progresso tecnico, la natura dei dati, le specifiche caratteristiche del trattamento, in modo da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve adottare misure tecniche e organizzative idonee a salvaguardare la sicurezza dei suoi servizi, l'integrità delle comunicazioni elettroniche e dei dati relativi al traffico e di quelli relativi all'ubicazione.

Misure minime: complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dal codice.

Notificazione: comunicazione al Garante, una sola volta ed esclusivamente per via telematica, di determinate tipologie di utilizzo dei dati, in gran parte sensibili. L'obbligo di notificazione è diventato più snello: l'Authority ha recentemente chiarito i confini dell'adempimento individuando i casi di esonero.

Obblighi di sicurezza: i dati personali oggetto di trattamento sono custoditi e controllati, in linea con il progresso tecnico, mediante l'adozione di misure di sicurezza idonee e preventive, per ridurre al minimo i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

Ospedali: ammesso il monitoraggio dei pazienti ricoverati in particolari reparti, come, ad esempio la rianimazione. Alle immagini possono accedere personale autorizzato e familiari dei ricoverati in reparti dove non sia consentito recarsi personalmente.

Quesiti: è possibile inviare al Garante della privacy richieste di informazioni e quesiti, contattando l'ufficio relazioni con il pubblico sito in Piazza Montecitorio n.121, 00186 Roma. L'ufficio risponde dal lunedì al venerdì, dalle ore 10 alle ore 13 al seguente numero di telefono 06 696771, è anche possibile contattare il Garante via internet alla seguente e-mail: [garante@gpdp.it](mailto:garante@gpdp.it), o [urp@gpdp.it](mailto:urp@gpdp.it), PEC: [protocollo@pec.gpdp.it](mailto:protocollo@pec.gpdp.it).

Reclamo: si può proporre al Garante un reclamo circostanziato per rappresentare una violazione della disciplina in materia di trattamento dei dati personali. Il reclamo è sottoscritto dagli interessati o da associazioni che li rappresentano ed è presentato al Garante senza particolari formalità.

Rete pubblica di comunicazione: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico.

Reti di comunicazione elettronica: sistemi di trasmissione, apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo tramite radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici. Sono incluse le reti satellitari, terrestri mobili e fisse a commutazione di circuito e di pacchetto, compreso internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato.

Rettifica: diritto da parte della persona che ha consentito il trattamento dei propri dati, di ottenere la correzione dei dati personali inesatti.

Ricorso: i diritti di accesso, aggiornamento, rettifica e cancellazione di dati personali possono essere fatti valere con ricorso al Garante, che non può essere proposto se è stata già adita l'autorità giudiziaria.

Tecnologie biometriche: sistemi con cui si identificano le persone in base ad alcune caratteristiche fisiche. Dalle impronte digitali all'iride, dalla retina al volto, al Dna.

URP: l'ufficio relazioni con il pubblico del Garante della privacy.

Utente: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

Videocitofoni: insieme degli apparecchi che rilevano immagini o suoni senza registrazione sono ammissibili per identificare chi entra in luoghi privati. In genere sono dislocati all'ingresso di immobili in corrispondenza di campanelli con la finalità di controllare gli accessi ai visitatori. La loro esistenza deve essere resa nota tramite un'informativa agevolmente rilevabile, quando non sono utilizzati per fini strettamente personali.

Videosorveglianza: trattamento di dati personali effettuato con strumenti elettronici di rilevamento di immagini. L'installazione di telecamere è lecita solo se è proporzionata agli scopi che si intendono perseguire: gli impianti devono essere attivati solo quando altre misure (sistemi di allarme, controlli fisici e logistici, misure di protezione degli ingressi) siano realmente insufficienti o inattuabili. L'eventuale conservazione di immagini deve essere limitata nel tempo. Il cittadino deve sempre essere informato se un'area è sottoposta a videosorveglianza, tramite un cartello con simbolo che indica che l'area è controllata. In caso di digitalizzazione delle immagini o di videosorveglianza che valuti percorsi e lineamenti (ad esempio, il riconoscimento facciale) è obbligatorio sottoporre il sistema alla verifica preliminare dell'Authority. Un provvedimento generale del Garante della privacy varato il 20 maggio stabilisce regole precise, in linea con gli orientamenti comunitari. L'uso illecito dei sistemi di videosorveglianza espone a provvedimenti di blocco, sanzioni amministrative e penali.

ZTL: per i contrassegni di accesso alle zone a traffico limitato dei centri storici il codice della privacy ha introdotto una specifica norma: devono essere esposti sui veicoli e contenere solo i dati indispensabili a individuare l'autorizzazione rilasciata senza apposizione di simboli e diciture. Generalità e indirizzo della persona fisica interessata non devono essere direttamente visibili sul contrassegno. Per il trattamento dei dati raccolti mediante impianti di rilevazione degli accessi di veicoli nei centri storici e alle zone a traffico limitato si applicano le disposizioni del DPR 250/1999. I comuni per introdurre sistemi di rilevazione degli accessi dei veicoli ai centri storici e a traffico limitato devono chiedere una specifica autorizzazione amministrativa e limitare la raccolta dei dati sugli accessi rilevando le immagini solo in caso di infrazione.

I dati possono essere conservati solo per il periodo necessario a contestare le infrazioni e a definire il relativo contenzioso. Si può accedere a questi dati solo ai fini di polizia giudiziaria o di indagine penale.

## **§.5 - DATI GENERALI DELL'AZIENDA**

Azienda: Comune di Monte di Procida (NA)

Amministratore: Dott. Giuseppe Pugliese (SINDACO)

Sede legale: Via Panoramica; 80070 Monte di Procida (NA)

Sede operativa: Via Panoramica; 80070 Monte di Procida (NA)

Codice fiscale e partita IVA: 80100130634.

## **§.6 – STRUTTURAZIONE DELL'AZIENDA**

L'Azienda è strutturata con i seguenti uffici:

- Affari Generali, Ufficio di segreteria, Ufficio protocollo, Sport.
- Gare, Patrimonio, Demanio.
- Lavori pubblici, Urbanistica, Edilizia, Protezione Civile, Acquedotto, Fogne.
- Tributi, Pubblicità ed Affissioni, Commercio ed Attività Produttive, CED ed Innovazione Tecnologica.
- Bilancio, Ragioneria.
- Anagrafe, Stato Civile, Elettorale, Toponomastica, Economato, Personale.
- Servizi Sociali, Turismo e Cultura, Cimitero.
- Avvocatura, Contenzioso, Datore di Lavoro, Tutela Dati Personali.

- Polizia Municipale, Viabilità e Parcheggi, Randagismo, Trasporti.
- Igiene Urbana, Salute, Pubblica Istruzione, Sport e tempo libero.
- Ufficio Tecnico III.

## **§.7 – DESCRIZIONE DEL CICLO LAVORATIVO**

Il lavoro svolto dal Comune in intestazione del presente DPS è diviso per reparto:

- ❖ Affari Generali, Ufficio di segreteria, Ufficio protocollo, Sport: riceve documenti dall'esterno o fa partire documenti per altre destinazioni tramite protocollo, si occupa delle attività del Comune tramite gli affari generali e con ufficio di segreteria riceve pubblico.
- ❖ Gare, Patrimonio, Demanio: si occupa di gare pubbliche demandando a ditte vincitrici di gare, gestiscono il patrimonio del Comune ovvero i beni strumentali e immobili.
- ❖ Lavori pubblici, Urbanistica, Edilizia, Protezione Civile, Acquedotto, Fogne: si occupa di gestire il bene pubblico quali strade, viabilità, gestione delle fogne e del bene acqua che forniscono a tutti gli abitanti, gestisce il patrimonio edilizio proprio e regolarizzando lavori o costruzioni a mezzo dell'ufficio edilizia.
- ❖ Tributi, Pubblicità ed Affissioni, Commercio ed Attività Produttive, CED ed Innovazione Tecnologica: si occupa di far pagare tributi quali TARI, IMU, etc., gestisce e regola la pubblicità e le affissioni in modo regolare, e si occupa del rilascio delle autorizzazioni sindacali a tutte le attività commerciali sul proprio territorio.
- ❖ Bilancio, Ragioneria: si occupa del bilancio annuale e previsionale del Comune gestendo anche i pagamenti del personale e di eventuali contratti in essere per manutenzioni o forniture di beni e servizi.

- ❖ Anagrafe, Stato Civile, Elettorale, Toponomastica, Economato, Personale: gestisce la popolazione, nascite, morti, rilascio di certificati e di documenti di identità, cura la viabilità a mezzo di eventuale cambio di nominativo di strade o gestire le mappe con le costruzioni aggiornate, ha voce in capitolo su spese da effettuare tramite l'economato e gestisce anche il personale quale aggiornamento qualifiche, scatti di carriera e gestione contributi con INPS, INAIL.
- ❖ Servizi Sociali, Turismo e Cultura, Cimitero: gestione di situazioni sociali difficili che hanno il contributo anche di assistente sociale con il quale il Comune ha una convenzione, si occupa della promozione e visibilità del Comune a favore di turisti, promuove la cultura sul proprio territorio con mostre, incontri, convegni, gestisce la parte cimiteriale a mezzo di cappelle e terreno per interro dei defunti del proprio Comune.
- ❖ Avvocatura, Contenzioso, Datore di Lavoro, Tutela Dati Personali: gestione delle controversie che possano nascere con altri enti pubblici o con privati, gestione del datore di lavoro (sindaco) a mezzo di atti per la salvaguardia del datore di lavoro e gestione di tutta la parte della privacy che riguardano dati di qualsiasi tipo trattati all'interno del Comune.
- ❖ Polizia Municipale, Viabilità e Parcheggi, Randagismo, Trasporti: gestione della viabilità e della regolarizzazione del traffico in alcuni punti e orari, rispetto dei parcheggi su strisce blu o di infrazioni effettuate al codice della strada, si occupa di gestire il randagismo con cani abbandonati, recuperandoli e inserendoli in canili municipali, si occupa del ramo trasporti all'interno delle zone di competenza del proprio Comune, gestendo la viabilità di trasporti eccezionali o particolari e anche della viabilità ordinaria delle autovetture e delle condizioni delle strade.

- ❖ Igiene Urbana, Salute, Pubblica Istruzione, Sport e tempo libero: gestisce la sanità pubblica ovvero la tutela della salute della popolazione del Comune, con attivazioni di monitoraggi di acque, etc., gestiscono le scuole afferenti al Comune con mensa e diritto allo studio degli adolescenti, tratta in particolare buoni pasto anche per bambini disagiati, promuove lo sport sul territorio con iniziative comunali e spazi comunali dove poter accogliere i bambini e i giovani del territorio (parchi, giardini, etc.).
- ❖ Ufficio Tecnico III: si occupa della gestione delle pratiche amministrative relative al pubblico e al privato con visione di elaborati relativi a ristrutturazioni di appartamenti o edifici anche di pregio storico, indicando e indirizzando secondo le norme vigenti senza rischiare abusi edilizi.

### §.7.1 – Elenco degli incaricati al trattamento

Le persone incaricate al trattamento dei dati sono individuate nelle figure di:

1. dirigente Affari Generali, Ufficio di segreteria, Ufficio Protocollo, Sport, Igiene Urbana, Salute, Pubblica Istruzione, Sport e tempo libero: dott.ssa GIOVANNA ROMEO, dirigente,

dipendenti del settore:

- ✓ sig.ra Elvira D’Agostino, segreteria, affari generali,
- ✓ sig. Francesco Prisco, messo comunale,
- ✓ sig. Vincenzo Lubrano Lavadera, segreteria affari generali,
- ✓ sig. Giuseppe Illiano, segreteria affari generali,
- ✓ sig. Raffaele Schiano Lomoriello, centralino,
- ✓ sig. Giacomo A. Guardascione, protocollo.

- Gare, Patrimonio Demanio: arch. ANTONIO ILLIANO, dirigente,

dipendenti del settore:

- ✓ geom. Michele Aquilone, demanio-patrimonio,
- ✓ sig. Antonio di Stasio, demanio,
- ✓ sig. Roberto Marino, gare-anticorruzione,
- ✓ sig.ra Maria Orsini, gare-anticorruzione.

- Lavori Pubblici, Urbanistica, Edilizia, Protezione Civile, Acquedotto, Fogne: ing. SALVATORE ROSSI, dirigente,

dipendenti del settore:

- ✓ arch. Antonio Illiano, edilizia privata,
- ✓ sig. Biagio Vicidomini, servizio idrico,
- ✓ sig. Maria Dello Ioio, servizio idrico,
- ✓ ing. Antonio Ferrante, lavori pubblici,
- ✓ geom. Francesco Anzalone, fogne,
- ✓ geom. Mario De Santis, edilizia privata,
- ✓ geom. L. Tobia Parascandolo, edilizia privata,
- ✓ sig. Carmine Russo, operaio,
- ✓ sig. antonio Silvestri, operaio,
- ✓ sig. Aldo Carannante, operaio.

- Tributi, Pubblicità ed Affissioni, Commercio ed Attività Produttive, CED ed Innovazione Tecnologica: sig. MARIO SCAMARDELLA, dirigente.

- Bilancio, Ragioneria: dott.ssa MICHELA DI COLANDREA, dirigente,

dipendenti del settore:

- ✓ sig.ra Silvana Angela Prodigio, ragioneria.

- Anagrafe, Stato civile, Elettorale, Toponomastica, Economato, Personale: dott.ssa CONCETTA SCUOTTO, dirigente,

dipendenti del settore:

- ✓ sig. Domenico Costagliola, elettorale,
- ✓ sig. Francesco Vecchione, anagrafe,
- ✓ sig.ra Fiorella Carannante, anagrafe,
- ✓ sig. Antonio Carannante, stato civile,
- ✓ sig. Giuseppe Spinelli, personale.

- Servizi Sociali, Turismo e Cultura, Cimitero: sig. ANTONIO CAPUANO, dirigente,

dipendenti del settore:

- ✓ sig. Francesco Merone, cimitero,
- ✓ sig. Francesco Illiano, cimitero,
- ✓ sig.ra Antonietta Schiano Lomoriello, servizi sociali,
- ✓ sig.ra Anna Scotto Di Carlo, servizi sociali,
- ✓ sig. Giuseppe Cangiano, servizi sociali.

- Avvocatura, Contenzioso, Datore di Lavoro, Tutela Dati Personali: avv. CIRO PUGLIESE, dirigente.

- Polizia Municipale, Viabilità e Parcheggi, Randagismo, Trasporti: dott. UGO MANCINO, dirigente,

dipendenti del settore:

- ✓ sig. Filiberto Emanato, segnaletica, viabilità, parcheggi,
- ✓ sig. Nunzio Castiglia, vigilanza,
- ✓ sig. Vincenzo Illiano, polizia giudiziaria,
- ✓ sig. Virgilio Scamardella, vigilanza,
- ✓ sig. Ciro Lomoriello Schiano, ufficio contravvenzioni,
- ✓ sig. Vincenzo Scotto di Cesare, vigilanza,
- ✓ sig. Salvatore Barone, vigilanza,
- ✓ sig. Antonio Guardascione, vigilanza,
- ✓ sig. Nislao Della Ragione, segreteria comando,
- ✓ sig. Francesco Della Ragione, polizia amministrativa,
- ✓ sig.ra Giuseppina Lubrano, vigilanza,
- ✓ sig. Giuseppe Carannante, operaio.

## **§.8 – TITOLARE DEL TRATTAMENTO (art. 24 UE 679/2016)**

Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento Europeo 679/2016.

Il Titolare del trattamento è persona giuridica o fisica, che ha la responsabilità di tutta la gestione del trattamento di tutti i tipi di dati che vengono trattati al proprio interno.

## **§.9 – RESPONSABILE DEL TRATTAMENTO (art. 28 UE 679/2016)**

Il Responsabile del trattamento deve garantire che metta in atto sufficienti misure e tecniche organizzative adeguate il modo tale che il trattamento soddisfi i requisiti del regolamento europeo e della legislazione italiana.

I trattamenti da parte del Responsabile del trattamento sono disciplinati da un contratto che vincola il responsabile del trattamento al titolare del trattamento con il quale si disciplina la durata del trattamento, la natura, la finalità del trattamento, il tipo di dati trattati e le categorie interessate.

Il Responsabile del Trattamento deve garantire che le persone autorizzate al trattamento dei dati trattati si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

Deve applicare quanto riportato all'art. 32 del Regolamento 679/2016.

Garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre cose:

- a) garantire la pseudonimizzazione e la cifratura dei dati trattati,
- b) capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento,

- c) capacità di ripristinare rapidamente la disponibilità e l'accesso ai dati trattati in caso di incidente fisico o tecnico,
- d) procedura per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative per garantire la sicurezza dei dati trattati.

## **§.10 – RESPONSABILE DELLA PROTEZIONE DEI DATI**

### **(art. 37 UE 679/2016)**

Il Responsabile della Protezione dei Dati (RPD) viene designato dal Titolare del trattamento e dal Responsabile del trattamento quando:

- a) il trattamento è effettuato da un organismo pubblico,
- b) il trattamento dei dati consistono in trattamenti che per loro natura, ambito di applicazione e finalità richiedono il monitoraggio regolare e sistematico degli interessati.

Il Titolare del trattamento e il Responsabile del trattamento assicurano che l'RPD sia coinvolto in tutte le questioni riguardanti la protezione dei dati trattati; lo sostengono nell'esecuzione dei compiti fornendogli risorse necessarie per assolvere i propri compiti.

Gli interessati ai dati trattati si rivolgono all'RPD per questioni relative al trattamento dei dati ed esercitano i loro diritti derivanti dal Regolamento.

E' tenuto al segreto e alla riservatezza dei propri compiti durante l'esercizio delle propri funzioni.

I suoi compiti sono:

- 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 presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

- b) Sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri 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;
- d) Cooperare con l'autorità di controllo; e
- e) 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.

## **§.11 – ELENCO DEI TRATTAMENTI DI DATI POSTI IN ESSERE DAL TITOLARE DEL TRATTAMENTO**

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.

Ogni banca dati o (archivio) deve essere classificato in relazione alle informazioni in essa contenute indicando se si tratta di dati personali, dati sensibili.

Per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato apposito modulo, che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro.

Viene di seguito riportato l'elenco dei trattamenti e il tipo di strumento impiegato per trattare tali dati e le modalità messe in essere dal Titolare del trattamento.

<b>Banca dati</b>	<b>Tipo di trattamento</b>	<b>Strumento utilizzato</b>
01	Elenco e trattamento dei dati personali	Archivio Cartaceo Archivio Elettronico
02	Elenco e trattamento dei dati sensibili	Archivio Cartaceo Archivio Elettronico
03	Elenco e trattamento dei dati giudiziari	Archivio Cartaceo Archivio Elettronico

### §.11.1 – Informazioni essenziali sull'elenco dei trattamenti

Viene di seguito riportata tabella con informazioni essenziali ai tipi di dati trattati.

Tabella 1 – informazioni essenziali sull'elenco dei trattamenti

legenda: P = dati personali – S = dati sensibili – G = giudiziari

Sede del trattamento		Natura dei dati trattati			Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	P	S	G		

**COMUNE DI MONTE DI PROCIDA – Via Panoramica**  
**DOCUMENTO PROGRAMMATICO SICUREZZA DEI DATI**

Affari Generali, Ufficio di Segreteria, Ufficio protocollo, Sport	Utenti Personale	X				Archivio cartaceo Archivio elettronico
Gare, Patrimonio, Demanio	Utenti	X		X		Archivio cartaceo Archivio elettronico
Lavori Pubblici, Urbanistica, Edilizia, Protezione Civile, Acquedotto, Fogne	Utenti	X		X	Acquedotto Halley Campania s.r.l.	Archivio cartaceo Archivio elettronico
Tributi, Pubblicità e Affissioni, Commercio ed Attività Produttive, CED ed Innovazione Tecnologica	Utenti	X		X	Acquedotto Halley Campania s.r.l.	Archivio cartaceo Archivio elettronico

**COMUNE DI MONTE DI PROCIDA – Via Panoramica**  
**DOCUMENTO PROGRAMMATICO SICUREZZA DEI DATI**

Bilancio, Ragioneria	Utenti Personale	X	X	X	Halley Campania s.r.l.	Archivio cartaceo Archivio elettronico
Anagrafe, Stato Civile, Elettorale, Toponomastica, Economato, Personale	Utenti Personale	X	X	X	Maggioli Informatica	Archivio cartaceo Archivio elettronico
Servizi Sociali, Turismo e Cultura, Cimitero	Utenti	X	X	X	Assistente Sociale (Dott.ssa Mafalda Guardascione)	Archivio cartaceo Archivio elettronico
Avvocatura, Contenzioso, Datore di Lavoro, Tutela Dati Personalizzati	Utenti Personale	X	X	X	Professionisti Esterni RPD privacy	Archivio cartaceo Archivio elettronico
Polizia Municipale, Viabilità e Parcheggi, Randagismo, Trasporti	Utenti Personale	X		X	Concilia Maggioli Informatica	Archivio cartaceo Archivio elettronico

Igiene Urbana, Salute, Pubblica Istruzione, Sport e Tempo Libero	Utenti	X	X			Archivio cartaceo Archivio elettronico
Ufficio Tecnico III	Utenti	X		X		Archivio cartaceo Archivio elettronico

## **§.12 – REGISTRI DEL TRATTAMENTO DEI DATI (art. 30 UE 679/2016)**

Devono essere istituiti dal titolare del trattamento o dal suo rappresentante con le attività di trattamento svolte e dal Responsabile del Trattamento. Tali registri devono contenere le seguenti informazioni:

- a) Il nome e i dati del contatto del titolare del trattamento, del responsabile del trattamento e del responsabile della protezione dei dati;
- b) Le finalità del trattamento;
- c) Descrizione delle categorie di interessati e delle categorie dei dati trattati;
- d) Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- e) Termine ultimo per la cancellazione delle diverse categorie di dati trattati;
- f) Descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'art. 32 del Regolamento ovvero pseudonimizzazione , cifratura, ripristino dei dati, etc.

## **§.13 – CARATTERISTICHE DELLE AREE E DEI LOCALI, NONCHE’ DEGLI STRUMENTI CON CUI SI EFFETTUANO I TRATTAMENTI**

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l’elenco delle sedi in cui viene effettuato il trattamento dei dati.

Per redigere l’inventario delle sedi in cui vengono trattati i dati deve essere utilizzato apposito modulo che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro.

### **§.13.1 – Ubicazione degli strumenti per il trattamento dei dati**

I locali dove vengono eseguiti trattamento di dati sono:

1. Affari Generali, Ufficio di segreteria, Ufficio protocollo, Sport locali dove vi sono sempre impiegati del settore, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale.
2. Gare, Patrimonio, Demanio: locali dove vi sono sempre impiegati del settore, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale.
3. Lavori Pubblici, Urbanistica, Edilizia, Protezione Civile, Acquedotto, Fogne: locali dove vi sono sempre impiegati del settore, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale.
4. Tributi, Pubblicità e Affissioni, Commercio ed Attività Produttive, CED ed Innovazione Tecnologica: locali dove vi sono sempre impiegati del settore, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale.
5. Bilancio, Ragioneria: locali dove vi sono sempre impiegati del settore, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale.

6. Anagrafe, Stato Civile, Elettorale, Toponomastica, Economato, Personale: locali dove vi sono sempre impiegati del settore, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale.
7. Servizi sociali, Turismo e Cultura, Cimitero: locali dove vi sono sempre impiegati del settore, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale.
8. Avvocatura, Contenzioso, Datore di Lavoro, Tutela Dati Personali: locale dove o vi è il dirigente responsabile o il settore è chiuso a chiave, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale.
9. Polizia Municipale, Viabilità e parcheggi, Randagismo, Trasporti: locali dove vi sono sempre impiegati del settore, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale; il locale archivio si trova al piano interrato.
10. Igiene Urbana, Salute, Pubblica, Istruzione, Sport e Tempo Libero: locali dove vi sono sempre impiegati del settore, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale.
11. Ufficio Tecnico III: locali dove vi sono sempre impiegati del settore, gli armadi sono chiusi con documenti, i personal computer sono ad accesso singolo con password individuale.

### §.13.2 – Elenco degli strumenti per il trattamento dei dati

E' compito del Responsabile del trattamento dei dati tenere aggiornato l'elenco degli strumenti adoperati per il trattamento dei dati.

L'elenco degli strumenti utilizzati è riportato di seguito:

- vengono utilizzate modulistiche approntate per ogni tipo di servizio e necessità; per l'archivio elettronico vengono utilizzati personal computer ad accesso singolo con username e password individuale, tutti collegati con un server che garantisce accesso a tutti gli utenti collegati alla rete intranet interna; durante l'impiego dei personal computer vengono utilizzati anche programmi licenziati per la gestione di attività e servizi particolari (anagrafe, contravvenzioni, etc.).

## **§.14 – ANALISI DEI RISCHI CHE INCOMBONO SUI DATI**

Il luogo di conservazione individuato per l'archivio è l'armadio ad ante in Direzione, deve essere protetto da:

- agenti chimici,
- fonti di calore,
- intrusioni ed atti vandalici,
- incendio,
- allagamento,
- furto.

Il rischio che incombe sui dati trattati è ad un livello medio, in quanto i locali che ospitano l'archivio cartaceo di ogni singolo settore del Comune è protetto da persone estranee.

Nei locali del Comune vi è sempre presenza di personale che sovrintende alle attività di trattamento dati, non lasciando mai gli uffici scoperti di personale.

Si riporta di seguito tabella specifica con analisi sui rischi esistenti sui dati trattati.

Tabella 3 – analisi dei rischi

Rischi		Si/No	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
Comportamento degli operatori	Sottrazione parziale dell'archivio o di documenti	SI	BASSA
	Carenza di consapevolezza, disattenzione o incuria	SI	ALTA

**COMUNE DI MONTE DI PROCIDA – Via Panoramica**  
**DOCUMENTO PROGRAMMATICO SICUREZZA DEI DATI**

	Comportamenti sleali o fraudolenti	NO	ALTA
	Errore materiale	SI	MEDIA
	Altro evento	NO	BASSA
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	SI	MEDIA
	Sottrazione di documenti contenenti dati	NO	BASSA
	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	SI	MEDIA
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	SI	BASSA
	Errori umani nella gestione della sicurezza fisica	SI	BASSA
	Altro evento	NO	BASSA

## **§.15 – MISURE DA ADOTTARE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI**

Il Responsabile del trattamento dei dati deve garantire l'integrità e disponibilità dei dati, ovvero deve garantire che gli stessi non vengano alterati, e soprattutto deve assicurare che i dati siano disponibili in ogni momento se ne renda necessaria la consultazione.

Il Responsabile del trattamento dei dati deve definire le modalità di accesso ai locali in cui è presente l'archivio ai dati trattati.

Il Responsabile del trattamento dei dati deve informare con una comunicazione scritta l'incaricato del locale dei compiti che gli sono stati affidati utilizzando apposito modulo.

### **§.15.1 – La protezione delle aree e dei locali**

Il Responsabile del trattamento deve regolamentare l'accesso al locale dove esiste l'archivio cartaceo.

L'accesso al locale dove c'è l'archivio deve essere rigido e comunque non si deve dare l'opportunità a persone estranee di poter accedere a tale locale facilmente.

### **§.15.2 – L'archiviazione e custodia di atti e documenti**

Il Responsabile del trattamento deve far sì che i dati personali e sensibili in forma cartacea debbano essere custoditi presso armadi o cassetti non accessibili a tutti gli operatori e soprattutto a persone estranee alle attività. L'accesso all'archivio cartaceo è controllato dallo stesso Responsabile del trattamento e dal socio impiegato, che ne curano accessi e modalità ai dati sensibili.

### **§.15.3 – Le misure logiche di sicurezza**

Il Responsabile del trattamento deve mettere in atto misure di sicurezza adeguate a far sì che nessuna persona estranea o non autorizzata possa accedere ai dati sensibili.

Devono essere adottate le seguenti misure:

- autenticazione dell'incaricato: l'incaricato del trattamento deve essere identificato e registrato su apposito modulo tenuto dal responsabile;
- controllo degli accessi: gli accessi al locale dove esiste l'archivio cartaceo deve essere vigilato dallo stesso Responsabile del trattamento o dallo stesso personale;
- annotazione del responsabile dell'operazione: dovrebbe essere creato un registro in cui riportare le persone che hanno accesso a documenti sottoposti a riserva.

## **§.16 – CRITERI E MODALITA' DI RIPRISTINO DEI DATI, IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO**

Il Responsabile del trattamento dei dati deve garantire il ripristino dei dati in caso di distruzione o danneggiamento dei dati stessi.

In particolare essendo l'archivio cartaceo, l'unico archivio detenuto per ogni singolo settore, non esistono copie di riserva, a meno che il responsabile non faccia fotocopia di atti delicati e particolari.

Potrebbe essere approntata la scansione di tutti i documenti di archivio in modo da aver una gestione migliore anche in caso di ricerca futura su pratiche vecchie.

Per quanto riguarda i PC essi sono protetti con firewall, antivirus e per copia di riserva, la stessa viene effettuata su hard disk esterno posizionato in locale protetto da agenti fisici o evento anomalo e fruibile in caso di perdita di tutti i dati afferenti sul server.

## **§.17 – ANALISI DEL MANSIONARIO PRIVACY E DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI**

Il Responsabile del trattamento deve provvedere affinché siano seguiti i criteri del mansionario della privacy e soprattutto che vengano eseguiti corsi formativi nei confronti degli incaricati al trattamento ai fini della privacy.

### **§.17.1 – Il mansionario privacy**

Vengono descritti di seguito i seguenti criteri:

#### **L'articolazione dei responsabili con i loro compiti essenziali**

- a) Il Responsabile del trattamento dei dati è individuato nel dott. Giuseppe Pugliese, sindaco e rappresentante del Comune, addetto alla custodia e accesso all'archivio cartaceo ed elettronico (dati personali, dati sensibili, dati giudiziari).

### **§.17.2 – Le misure di sicurezza di carattere organizzativo**

Le misure di sicurezza vengono di seguito riportate.

#### **§.17.2.1 – Descrizione delle modalità di incarico del personale**

Il personale è incaricato secondo gli uffici e i servizi di competenza, e le competenze singole già sopra richiamate.

#### **§.17.2.2 – Conferma di aver impartito le prescrizioni in termini di sicurezza**

Saranno fornite agli incaricati del trattamento prescrizioni minime di sicurezza, sia a livello di igiene e sicurezza sul lavoro (D.Lgs. 81/2008 e s.m.i.) sia e soprattutto a livello di sicurezza dei dati con opuscolo consegnato ai singoli incaricati, in caso di presenza futura.

*§.17.2.3 – Conferma di aver adottato le procedure per la classificazione dei dati*

I dati trattati dal Comune vengono custoditi in armadi chiusi a chiave e sempre vigilati durante gli orari di lavoro e soprattutto durante l'apertura degli uffici al pubblico; i personal computer sono in protezione da eventuale furto da parte di pubblico afferente agli uffici, in quanto ogni PC ha username e password individuale per l'accesso e ogni dipendente prima di alzarsi dal proprio posto di lavoro fa partire il salvaschermo che non consente di poter accedere alla postazione se non a mezzo password individuale.

*§.17.2.4 – Prescrizioni di linee-guida di sicurezza e altre istruzioni interne*

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- Il responsabile del trattamento autorizza preventivamente coloro i quali sono individuati al trattamento dei dati.
- Obbligo di non lasciare incustodito e accessibile l'archivio cartaceo, durante una sessione di trattamento, neppure in ipotesi di breve assenza.
- Obbligo dell'incaricato di far sì che nessuna persona estranea al trattamento possa avere accesso ai dati o documenti.
- Almeno annualmente viene aggiornato l'elenco degli incaricati a cura del responsabile del trattamento, tale elenco viene custodito dallo stesso responsabile del trattamento.
- Durante una sessione di trattamento dati, è fatto divieto all'incaricato o al responsabile, di far accedere nelle aree dove avviene il trattamento, qualsiasi persona estranea che possa interferire con l'archivio cartaceo o possa venire in possesso di notizie riservate.
- Eventuali persone estranee al trattamento devono essere autorizzate preventivamente dal Responsabile, che viene identificata e registrata.

- E' fatto divieto al responsabile e agli incaricati durante la routine lavorativa, di non avere mai sulla scrivania documenti o carte riconducibili a pazienti diversi da quello che si sta trattando in quel momento.
- Alla fine della sessione del trattamento l'incaricato di concerto con il responsabile del trattamento ripongono eventuale documentazione ancora fuori archivio.
- Eventuale personale che possa accedere oltre gli orari di lavoro (personale di pulizia), devono essere identificati e registrati preventivamente, e sempre allorquando vi sia cambiamento di personale che si occupi delle pulizie.
- Inoltre devono essere identificati e registrati il personale di pulizia che si trovino ad entrare nell'area in cui è contenuto l'archivio cartaceo.
- Qualsiasi manomissione avvenga nell'archivio cartaceo, unica responsabilità sarà del responsabile del trattamento e dell'incaricato, il quale dovranno aver curato bene la sicurezza dell'archivio cartaceo contenuto in armadio chiuso con la chiave in loro possesso.

I dati personali e sensibili degli utenti sono trattati direttamente dagli incaricati di ogni servizio e ufficio, lo stesso dicasi per il trattamento dei dati personali, sensibili e giudiziari dei dipendenti.

In particolare i dati sensibili e giudiziari in possesso del Comune, devono essere custoditi in luoghi non accessibili a chiunque, e conservati in cassetti o armadi che siano possibilmente ignifughi (a prova di fuoco), i quali possano garantire durante un evento dannoso un tempo per poter mettere in salvo l'archivio cartaceo.

### §.17.3 – I piani di formazione del personale

Gli incaricati del trattamento dei dati sia personali, sia sensibili, vengono sottoposti a regolare corso di formazione in base ai rischi esistenti durante il trattamento dei dati.

In particolare il Responsabile del trattamento controlla e vigila sul corretto svolgimento dei corsi di aggiornamento del personale nuovo assunto o del personale esistente.

I piani di formazione vengono stesi o dal datore di lavoro o anche dal RPD di concerto con il Responsabile del trattamento, per poi essere sottoposti e somministrati agli incaricati del trattamento dei dati.

## **§.18 – DESCRIZIONE DEI CRITERI DA ADOTTARE, PER GARANTIRE L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA, IN CASO DI TRATTAMENTI DI DATI PERSONALI E SENSIBILI AFFIDATI ALL'ESTERNO**

Il Responsabile del trattamento, in caso di affidamento a soggetti esterni del trattamento dei dati, deve provvedere alla nomina degli stessi come responsabili del trattamento dei dati personali.

I dati trattati vengono delegati anche a consulenti esterni o altri enti pubblici o privati a seconda del tipo di attività da svolgere.

L'RPD ha già elaborato modulistica nel caso di trattamento di dati esterni con altri enti o organi o con privati che possano venire a conoscenza di documenti o notizie.

## **§.19 – CONTROLLO PERIODICO SULLO STATO DELLA SICUREZZA**

Il Responsabile/Titolare del trattamento di concerto con il Responsabile della Protezione dei Dati cura gli adempimenti della privacy, monitora periodicamente lo stato di sicurezza del sistema di tenuta dell'archivio cartaceo e delle procedure instaurate ai fini del Codice della Privacy.

In particolare il Responsabile/Titolare del trattamento deve:

- adottare le misure idonee affinché non vi siano infrazioni al Codice della Privacy,
- di concerto con l'RPD che cura gli adempimenti della privacy, curare e monitorare ciclicamente tutto il processo che segue per il trattamento dei dati sia personali che sensibili, quando questi dati (in forma cartacea o telematica) vengono trasferiti a settori di altri enti pubblici o privati.

### **§.19.1 – Controlli di sicurezza**

Aspetto importante è quello sulla sicurezza del personale. Gli obiettivi sono:

- ridurre il rischio di errori umani, furto, frode o uso improprio delle strutture dell'organizzazione,
- accertarsi che gli utenti interni siano informati sulle minacce alla sicurezza delle informazioni e siano formati a sostenere le politiche di sicurezza nel corso della propria attività lavorativa,
- minimizzare il danno per incidenti e malfunzionamenti circa la sicurezza e mettere a frutto l'esperienza di avvenimenti precedenti.

## **§.20 – MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO**

Il Responsabile del trattamento deve mettere in essere tutte quelle misure che non consentano di trattare o venire a contatto con i dati personali o sensibili a nessun tipo di persona che non faccia parte degli incaricati al trattamento, e quindi di conseguenza si abbia un trattamento dei dati personali e sensibili non consentito.

Si riportano di seguito azioni da mettere in pratica per abbassare il potenziale rischio appena accennato.

### **§.20.1 – Personale autorizzato al trattamento dei dati**

Il Responsabile del trattamento deve redigere ed aggiornare ogni variazione dell'elenco degli incaricati autorizzati al trattamento dei dati sia personali che sensibili.

### **§.20.2 – Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni**

Nel caso di aggiornamento del personale o degli incaricati al trattamento, deve essere compilato apposito modulo da parte del Responsabile del trattamento e questo deve essere archiviato.

Il Responsabile del trattamento

Dott. GIUSEPPE PUGLIESE

---

Il consulente esterno

dott. ing. CARLO ZUDDAS

---