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

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 personal 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 instituita 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 dei 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, o urp@gpdp.it, PEC: 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.

Banca dati	**Tipo di trattamento**	**Strumento utilizzato**
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		

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

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 Personali	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 sovraintende 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		Sì/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

	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 si 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	Il consulente esterno
Dott. GIUSEPPE PUGLIESE	dott. ing. CARLO ZUDDAS
_____	_____