NapoliServizi

MANUALE DELLA SICUREZZA DELLE INFORMAZIONI NAPOLISERVIZI S.P.A.

AI SENSI DEL REGOLAMENTO EUROPEO (UE) 679/2016
E DEL CODICE PRIVACY (D.LGS.196/2003)

Disposizione Organizzativa n. 40 del 20/12/2018

Premessa

La Società per Azioni Napoli Servizi realizza, in regime di *in-house providing*, servizi integrati di Facility Management ed attività strumentali per conto del Comune di Napoli.

Secondo quanto riportato nello Statuto di Napoli Servizi S.p.A. (art. 3) "la società è strettamente necessaria al perseguimento delle finalità istituzionali del Comune di Napoli e assicura la produzione di beni e/o servizi di interesse generale, garantendo l'attuazione coordinata ed unitaria dell'azione amministrativa nonché un'organizzazione efficiente, efficace ed economica nell'ordinamento dell'ente locale, nel perseguimento degli obiettivi di interesse pubblico di cui il Comune è portatore. La società ha per oggetto la gestione, la valorizzazione e la dismissione del patrimonio immobiliare del Comune di Napoli e, inoltre, la prestazione di servizi di facility management ed attività strumentali esclusivamente nei confronti dell'Amministrazione comunale di Napoli e delle società totalmente partecipate dalla stessa amministrazione comunale e soggette al suo controllo analogo, con esclusione dei servizi pubblici locali con rilevanza economica".

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate e da adottare per il trattamento dei dati personali effettuato da Napoli Servizi S.p.A. (di seguito anche "Società" e "Napoli Servizi").

Occorre premettere che, in tema di tutela dei dati personali e della sicurezza del patrimonio informativo, la normativa italiana ha subito negli anni diverse evoluzioni.

A seguito dell'entrata in vigore del D.Lgs 196/2003 (Codice Privacy) e, specificatamente, ai sensi della regola 19 del Disciplinare Tecnico allegato b, tutti gli Enti erano tenuti alla redazione del Documento Programmatico della Sicurezza (DPS).
Con il Decreto Legge "Semplifica Italia" del 9 febbraio 2012, convertito nella legge n. 35 del 4 Aprile 2012, veniva invece abolito l'obbligo della tenuta ed aggiornamento del DPS e conseguentemente l'obbligo di menzionare tale Documento, ed i relativi aggiornamenti, nella relazione accompagnatoria al Bilancio di esercizio.
Restavano tuttavia invariate le altre misure di sicurezza – in particolare quelle previste dall'art. 34 del d.lgs. 196/2003 Codice Privacy, dal Disciplinare Tecnico, allegato b del Codice e dagli altri provvedimenti del Garante sul tema – misure che le aziende erano tenute ad osservare e porre in essere, al fine di tutelare il proprio patrimonio informativo.
Tali misure riguardano nello specifico:

- le misure minime descritte dall'art. 33 e ss. del Codice Privacy e nelle regole del Disciplinare tecnico (allegato B del Codice Privacy), onde assicurare un livello minimo di protezione dei dati personali;
- le misure adeguate di cui all'art. 31 del Codice Privacy, che le aziende debbono porre in essere in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento;
- le misure previste dal provvedimento del Garante del 27 novembre 2008 sugli Amministratori di Sistema.

Con l'entrata in vigore del Regolamento (UE) 2016/679, "Regolamento Generale per la Protezione dei Dati" (di seguito, anche "RGPD") applicabile in tutti gli Stati della Comunità Europea a decorrere dal 25 maggio 2018, la sicurezza delle informazioni è garantita ai sensi di quanto previsto dall'art.32 del Regolamento: ogni Titolare del trattamento è, pertanto, tenuto all'adozione di "adeguate misure tecniche e organizzative" funzionali atte a prevenire ed arginare i rischi del trattamento.

Pertanto, pur non essendo riportate, nel suddetto Regolamento, specifiche misure in tal senso, in base al principio di responsabilizzazione diretta del Titolare (cd. principio di accountabilty), costui è tenuto a determinare – in base ai trattamenti effettuati, alla natura dei dati ed alla propria struttura organizzativa- in che termini adottare "politiche e misure adeguate per garantire ed essere in grado di dimostrare che i trattamenti sono eseguiti conformemente al Regolamento" (art. 24 del Regolamento).

Da ultimo, con Decreto legislativo 10 agosto 2018, n.101 il Codice Privacy è stato completamente riformulato e sono stati abrogati sia il Titolo V "Sicurezza dei dati e dei sistemi" sia il Disciplinare tecnico (allegato B del Codice Privacy), pertanto, allo stato, fanno fede le prescrizioni del RGPD.

Sebbene nel RGPD non siano presenti riferimenti a specifiche misure di sicurezza da adottare, Napoli Servizi ha recepito quanto previsto dalla Circolare AgID n. 2/2017 del 18.04.2017 che sostituisce la Circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)» e che indica nell'allegato 1 tali misure, attuando le stesse in base al "modulo di implementazione" corrispondente all'allegato 2 della suddetta Circolare AgID.

Alla luce delle considerazioni fatte, il presente Manuale della Sicurezza delle informazioni è il documento che Napoli Servizi, quale Titolare del trattamento, ha inteso adottare allo scopo di verificare e monitorare il rispetto delle misure di sicurezza prescritte dal legislatore, misure atte a garantire la sicurezza della sede legale e delle sedi periferiche della società.

Nel documento vengono descritte nel dettaglio le politiche di sicurezza "adeguate" poste in essere, prendendo in considerazione anche le misure a suo tempo indicate dell'Allegato B del Codice Privacy che, unitamente alle misure per gli Amministratori di sistema, costituiscono ulteriori strumenti a supporto del sistema di sicurezza.

Sommario

1. Tipologie di trattamento dati personali

Al fine di elaborare quali tipologie di trattamenti sui dati sono posti in essere dal Titolare, si procede come segue:

- si individuano i tipi di dati personali trattati, in base alla loro natura (comuni, giudiziari o sensibili) ed alla categoria di soggetti cui essi si riferiscono (ad es. clienti, fornitori, personale);
- si individuano le aree nelle quali si effettuano i trattamenti dei dati;
- si differenziano i trattamenti nell'ambito delle attività aziendali di Napoli Servizi e quelli svolti per conto del Comune di Napoli.

1.1 Trattamenti aziendali

I trattamenti sui dati personali svolti all'interno di Napoli Servizi riguardano, in via principale, le operazioni degli stessi necessarie per dare corso alle attività aziendali.
I dati trattati dal Titolare nell'esercizio delle attività aziendali appartengono alle seguenti categorie di interessati:

- Candidati (dati comuni e categorie particolari di dati[1])
- Dipendenti (dati comuni, categorie particolari di dati e dati giudiziari[2])
- Fornitori / Consulenti (dati comuni)
- Organi societari (dati comuni, categorie particolari di dati e giudiziari)
- Inquilini degli immobili di proprietà del Comune di Napoli gestiti da Napoli Servizi (dati comuni, categorie particolari di dati e dati giudiziari)
- Contribuenti per pubbliche affissioni e pubblicità (dati comuni)

1.2 Trattamenti conto Terzi

Le informazioni gestite sono trattate solo dagli incaricati direttamente coinvolti nel trattamento e vengono archiviate, qualora necessario, secondo le modalità definite dalla Società con idonea procedura (in appositi archivi, cartacei e/o elettronici, ad accesso controllato).
Napoli Servizi S.p.A. eroga presso gli uffici del Comune di Napoli servizi di gestione dati di natura comune. Il personale incaricato alla gestione conto terzi è formato ed informato sui precetti del Decreto oggetto del presente documento. Si precisa che i requisiti di sicurezza di strutture e infrastrutture, da furto e incendio, nonché dalla distruzione accidentale dei dati sono oggetto di decisioni intraprese esclusivamente dal Comune di Napoli, che, in tale circostanza, opera quale Titolare dei dati. Il personale di Napoli Servizi è tenuto ad attenersi alle eventuali procedure di sicurezza trasmesse dal Comune-Titolare.

[1] Secondo la previsione legislativa, appartengono alle categorie particolari di dati personali i "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" (art. 9 comma 1 RGPD).
[2] Sono dati giudiziari, nello specifico, dati personali relativi a condanne penali e reati: i "dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza" (art. 10 RGPD).

2. Compiti e responsabilità nell'ambito delle strutture preposte al trattamento dei dati

Il trattamento dei dati avviene ad opera di personale definito ed autorizzato, secondo quanto stabilito Regolamento Europeo (UE) 679/2016 (di seguito, anche "RGPD") e dal D.lgs. 196/2003 (di seguito, anche "Codice Privacy"), come riformulato ai sensi del Decreto legislativo 10 agosto 2018, n.101.

L'azienda individua le figure preposte alla protezione dei dati personali e all'adozione di misure di sicurezza e gestione delle stesse, come di seguito elencate:

- **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 (art. 4 comma 1 punto. 7 RGPD);
- **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 (art. 4 comma 1 punto. 8 RGPD);
- **Responsabile della protezione dei dati**: soggetto designato dal Titolare che, dotato di specifiche competenze e responsabilità, deve essere coinvolto in tutte le questioni aziendali che interferiscono con la protezione dei dati personali, secondo quanto previsto dagli artt. 37 e ss. del RGPD;
- **Incaricati**: le persone fisiche sotto l'autorità del titolare o del responsabile autorizzate a compiere operazioni di trattamento ed istruite in tal senso (art. 29 RGPD e art. 2-quaterdecies comma 2 Codice Privacy);
- **Amministratori dei sistemi informatici:** sono i soggetti cui è conferito il compito di sovrintendere alle risorse di sistema operativo di un elaboratore o di un sistema di base di dati e di consentirne l'utilizzo.

2.1 Titolare del Trattamento

Il Titolare del trattamento esercita un potere decisionale autonomo sulle finalità e sulle modalità del trattamento dei dati personali in possesso all'azienda e contenuti nelle banche dati cartacee ed informatiche.

Il Titolare del trattamento ha pertanto il compito di adottare tutte le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, attraverso idonee istruzioni fornite per iscritto.

Il Titolare ha, inoltre, il compito di vigilare, anche tramite verifiche periodiche, sul rispetto delle proprie istruzioni, nonché sull'osservanza delle disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

2.2 Responsabile del Trattamento Dati

Il RGPD individua la figura dei Responsabili del trattamento dei dati personali all'art. 28, ma sembra principalmente orientato a regolamentare le condizioni relative ai soggetti terzi che svolgono operazioni di trattamento sui dati personali per contro del Titolare.

L'art. 2 quaterdecies del D.lgs. 196 del 2003, come riformulato dal Decreto legislativo 10 agosto 2018, n.101, invece dispone che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*".

Per dare attuazione agli adempimenti previsti dalla normativa in tema di protezione dati personali, l'Amministratore Unico di Napoli Servizi S.p.A. ha nominato il Rag. Mario Baggio, già Responsabile del Settore Affari Generali, quale Responsabile del Trattamento Dati (RTD) e, conseguentemente, Responsabile dell'Ufficio Privacy allo scopo costituito.
I compiti assegnati al suindicato RTD sono definiti nella delega conferita dall'Amministratore Unico, nella sua qualità di legale rappresentante di Napoli Servizi nonché di Titolare del trattamento.

Con riferimento ai soggetti terzi che, in base ad un contratto di fornitura di beni e servizi, svolgono operazioni di trattamento rilevanti per conto di Napoli Servizi ai sensi del citato art. 28 del RGPD, si conviene che essi possono essere nominati Responsabili del trattamento. Tali soggetti terzi, per quanto di propria competenza, sono tenuti per sé, per i propri dipendenti e per chiunque collabori con la loro attività, al rispetto della riservatezza, integrità e qualità dei dati e all'utilizzo esclusivo per le finalità specificate e definite nell'ambito del contratto in essere.
L'art. 28 del RGPD introduce importanti novità nel caso in cui alcuni trattamenti siano affidati dal Titolare a soggetti terzi; l'articolo in oggetto prevede espressamente che qualora "*un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato*".
Quindi la scelta del Responsabile deve ricadere su una persona fisica o giuridica che possieda specifiche competenze. Inoltre, l'esecuzione dei trattamenti per conto del titolare deve essere disciplinata da un contratto o da altro atto giuridico che vincoli Responsabile del Trattamento e Titolare del Trattamento all'osservanza di specifici obblighi normativi e contrattuali (obblighi meglio dettagliati nel testo normativo).

Il Responsabile esterno deve farsi carico di verificare che i dati personali oggetto di trattamento siano custoditi e controllati in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Egli deve inoltre accertarsi che siano adottate le misure di sicurezza previste dal RGPD e dalle procedure interne predisposte dal Titolare.
E' cura del Responsabile contribuire alla periodica valutazione del livello di adeguatezza complessivo della sicurezza, in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche dei trattamenti realizzati sotto la propria responsabilità.

Ai sub-Responsabili, laddove nominati – si ricorda che il RGPD introduce la figura del sub-responsabile quale soggetto a cui il Responsabile può affidare, previa autorizzazione scritta del

Titolare, alcune operazioni di trattamento – vanno trasferiti, con atto formale, gli stessi obblighi in materia di protezione dati personali previsti per Responsabile.

La Napoli Servizi S.p.A. si avvale della consulenza e del supporto esterno di fornitori terzi in diversi settori, (particolare rilievo – nell'ambito del Settore Servizi Informativi - rivestono i fornitori di supporti software e di assistenza hardware e software).
Per l'esecuzione dell'attività di cui sopra, sono stati stipulati regolari contratti accludenti i dettagli dei servizi offerti, è stata redatta la nomina del Responsabile del Trattamento e si è provveduto all'accertamento sull'utilizzo di misure idonee di sicurezza dei dati, secondo quanto disposto dalla normativa vigente.

2.3 Responsabile per la protezione dei Dati

Il Responsabile per la Protezione dei Dati è una nuova figura organizzativa introdotta ai sensi dell'art. 37 e ss. dal RGPD. L'istituzione del Responsabile per la Protezione dei Dati è considerata obbligatoria dal Regolamento solo per alcune categorie specifiche di Titolari e Responsabili. I Garanti Europei, comunque, incoraggiano tutti gli Enti, laddove possibile, a scegliere volontariamente di dotarsi di un RPD, in quanto figura importante per facilitare l'adeguamento alle previsioni del Regolamento.
La Napoli Servizi S.p.A., svolgendo una serie di attività per conto del Comune di Napoli ed essendo, pertanto, tenuta a nominare un Responsabile per la Protezione dei Dati ai sensi dell'art. 37 comma 1, ha individuato al suo interno tale figura. L'Amministratore Unico ha conferito con Determina n. 13 del 21/05/2018 all'avv. Angela Longobardi, l'incarico di Responsabile per la protezione dei dati ("RPD") ai sensi dell'art. 37 e ss. del Reg. (UE) n. 679/2016 del 27 aprile 2016.
I compiti assegnati al suindicato RPD sono definiti nella delega conferita dall'Amministratore Unico, quale legale rappresentante di Napoli Servizi, Titolare del trattamento.

2.4 Incaricati al Trattamento dei Dati

Sono i soggetti che, nello svolgimento della loro attività lavorativa presso Napoli Servizi svolgono materialmente operazioni di trattamento su dati, siano essi contenuti in banche dati informatiche o in archivi cartacei, sotto la diretta autorità del titolare, attenendosi alle istruzioni da esso impartite.
Vista la complessità della struttura organizzativa di Napoli Servizi, sono distinte tre tipologie di incarichi del trattamento dei dati personali:

Incaricati del trattamento di I° livello: sono individuati tra i responsabili di unità organizzative di primo livello e nominati con Disposizione Organizzativa del Titolare del Trattamento Dati. Gli incaricati di I° livello, rapportandosi costantemente con il RTD, provvedono, per le funzioni specificamente attribuite dall'atto di nomina, agli adempimenti imposti dal Regolamento Europeo 2016/679 del Codice Privacy
Incaricati del trattamento con funzioni di coordinamento: sono individuati tra i responsabili di unità organizzative di II° livello e sono chiamati a rapportarsi con l'incaricato di I° livello e, laddove necessario, con il RTD/ Ufficio Privacy o al RPD per tutte le questioni attinenti alla

gestione delle informazioni all'interno dell'unità organizzativa di appartenenza al fine di garantire gli adempimenti imposti dal Regolamento Europeo 2016/679 del Codice Privacy

Incaricati del trattamento: sono tutti i dipendenti che, con le disposizioni organizzative le operazioni di trattamento effettuate da tutti gli incaricati del trattamento, in esecuzione delle attività ad essi assegnate, devono svolgersi nel rispetto delle norme di legge, secondo le istruzioni impartite dal Titolare e dal RTD e per gli scopi propri della funzione organizzativa di appartenenza.

2.5 Amministratori di Sistema

Con la qualifica di Amministratori dei sistemi informatici, secondo il provvedimento del Garante del 27 novembre 2008, si devono identificare coloro che sono addetti alla gestione ed alla manutenzione di un impianto di elaborazione, costituito da sistemi, reti, basi dati; ma, sempre secondo il Garante, vanno considerati anche coloro che svolgono attività tecniche quali il salvataggio di dati, organizzazione delle strutture di rete, gestione dei supporti di memorizzazione, manutenzione hardware.

Per poter svolgere la funzione di Amministratori dei sistemi informatici, ai soggetti individuati (all'interno del Settore Servizi Informativi e tra i soggetti esterni che sono autorizzati ad operare sui sistemi aziendali) vengono concesse dal Titolare le "Autorità di sistema", che consistono nell'assegnazione di attributi, privilegi o accessi che consentono la gestione delle risorse del sistema operativo.

2.6 Mappa delle Responsabilità nel Trattamento dei Dati

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico con il quale è individuato puntualmente l'ambito del trattamento consentito. Di seguito si riportano le figure preposte in Napoli Servizi:

1. Titolare del trattamento dei dati: Napoli Servizi S.p.A., in persona dell'Amministratore Unico
2. Responsabile del trattamento dati: Rag. Mario Baggio, Responsabile funzionale del Settore Affari Generali e a capo dell'Ufficio Privacy di Napoli Servizi;
3. Responsabile per la protezione dei dati: avv. Angela Longobardi, che svolge la propria attività all'interno dello Segreteria di Staff del Direttore Generale;
4. Incaricati del trattamento dei dati: tutti i soggetti che svolgono attività di trattamento di dati comuni o sensibili sono stati nominati incaricati (distinti tra incaricati con funzioni di coordinamento e incaricati del trattamento).
5. Amministratori di Sistema: sono stati nominati il Responsabile del settore Servizi Informativi e tutti i soggetti che operano del settore.

Le lettere di nomina dei responsabili e quelle degli incaricati vengono raccolte ed ordinate in base all'unità organizzativa cui tali soggetti appartengono, in modo da restituire al Titolare un quadro chiaro ed esaustivo delle responsabilità, le attività in questione.

3. Analisi dei rischi che incombono sui dati

Il rischio a cui sono sottoposti i dati trattati da Napoli Servizi viene identificato prendendo in considerazione:

- la struttura del sistema informatico ed, in particolare, le risorse che costituiscono il sistema informatico aziendale e che, quindi, devono essere protette:

  - ✓ hardware primario (server);
  - ✓ hardware secondario (personal computer client);
  - ✓ software primario:
    - ➢ sistemi operativi del server,
    - ➢ gestore di base dati,
    - ➢ gestori di posta elettronica;
  - ✓ software secondario (sistemi operativi del client e applicativi di Office Automation);
  - ✓ supporti di memorizzazione dei dati;
  - ✓ trasmissioni dati;

- le regole comportamentali fornite agli operatori;
- gli archivi cartacei in cui sono presenti dati personali, e che quindi devono essere protetti.

Il livello di rischio viene rilevato, nello specifico, analizzando il livello di conformità alle misure minime di sicurezza di cui al disciplinare tecnico, allegato b del codice.

3.1 Dettaglio adeguamento alle misure standard

Le indagini condotte dai Sistemi Informativi aziendali sono state eseguite tenendo in considerazione, per quanto compatibili con il RGPD, l'adeguamento alle misure standard (prendendo in esame le regole già evidenziate dal disciplinare tecnico, allegato B del D.Lgs 196/2003, in quanto non in contrasto con le "misure adeguate" richieste dall'art. 32 del RGPD), le aree organizzative, le attività svolte dalla Società e le tipologie di rischio che possono gravare sui dati.

Sistema di autenticazione	
Applicata	Su tutte le postazioni di lavoro è attivo un sistema di autenticazione.
Credenziali di autenticazione	
Applicata	Ogni incaricato accede alla propria postazione di lavoro attraverso un'utenza associata ad una password, creata dal dipendente e non resa conoscibile a terzi.
Regola 3	**Utenze individuali**
Applicata	Le User_id utilizzate per l'accesso ai sistemi sono assegnate univocamente agli incaricati.
Segretezza delle credenziali	
Applicata	La segretezza e la custodia delle credenziali sono rimesse al buon senso e alla consapevolezza degli operatori. Specifiche regole comportamenti per il personale sono dettate nel "Regolamento informatico aziendale" che individua i criteri operativi per il corretto utilizzo degli strumenti informatici.
Caratteristiche delle credenziali	

Applicata	Esiste una regola specifica circa la lunghezza minima delle password; la periodicità del cambio password è fissata in tre mesi ed il cambio viene gestito dagli stessi sistemi informatici in uso. Il personale è informato circa le modalità per impostare la password: le regole operative da osservare sono contenute nel citato "Regolamento informatico aziendale".
Riutilizzo delle utenze	
Applicata	Le utenze vengono considerate personali ed incedibili, questo assunto vale anche nel caso che un incaricato venga sostituito per dimissioni o altro, pertanto il loro riutilizzo è vietato.
Scadenze delle utenze	
Applicata	Le utenze seguono direttamente l'incaricato a cui sono state assegnate. Pertanto, in caso di non utilizzo per dimissioni o altro, vengono disattivate.
Gestione utenze	
Parzialmente applicata	In concomitanza al cambio mansioni o abbandono del lavoro di un incaricato che comporti per lo stesso la perdita dei diritti di accesso ai dati, le utenze ad esso assegnate vengono disattivate (v. regola 7).
Workstation - istruzione per gli incaricati	
Applicata	Tutti i dipendenti sono sensibilizzati circa le regole operative e di sicurezza da osservare nell'utilizzo delle postazioni di lavoro, così come riportate nel "Regolamento informatico aziendale". Sulle postazioni, in caso di allontanamento prolungato, è attivo il blocco automatico della workstation.
Diritto di accesso da parte del titolare	
Applicata	Tutti gli incaricati sono a conoscenza dei diritti di accesso da parte del titolare. E' prevista una procedura finalizzata a garantire l'accesso ai dati da parte del Titolare in caso di prolungata assenza o impedimento di un Utente.
Sistema di autorizzazione	
Applicata	E' previsto un sistema di autorizzazione per gestire profili di accesso differenziati
Gestione profili di accesso ai dati	
Applicata	Sono definiti profili di autorizzazione, diversificati per aree e competenze; secondo necessità, si dispone che siano aggiunti o eliminati specifici diritti di accesso. I profili assegnati vengono revocati, in caso di cambio mansione, trasferimento o fine rapporto.
Verifiche periodiche dei profili di accesso	
Applicata	Periodicamente e, comunque, almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.
Aggiornamento periodico degli ambiti di accesso	

Applicata	Vedi "Verifiche periodiche dei profili di accesso"
Programmi di cui all'art. 615-quinquies del codice penale	
Applicata	Tutte le postazioni client sono dotate di software antivirus costantemente aggiornato per quanto riguarda le definizioni di nuovi virus.
Aggiornamenti periodici dei programmi	
Applicata	L'aggiornamento dei sistemi operativi e dei software in uso presso l'Azienda viene eseguito tramite una procedura che distribuisce gli aggiornamenti, anche tramite delle società fornitrici dei software. Gli aggiornamenti del software gestionale sono effettuati da personale interno stesso o tramite delle società fornitrici dei software.
Salvataggio dei dati	
Applicata	La copia dei dati avviene per tutte le banche dati utilizzate: il sistema di backup prevede una copia settimanale completa ed una copia giornaliera differenziale su nastri. Per backup completo si intende il backup di tutta la banca dati (database, file server, file di sistema). Per backup differenziale si intende quello relativo a tutti i cambiamenti effettuati a partire dall'ultimo backup completo. Sono presenti tecnologie di Disaster Recovery per la replica dei dati e dei server virtuali in siti remoti (Cloud) rispetto ai CED aziendali.
Situazioni cui all' art. 615-ter del codice penale	
Applicata	L'intera rete è protetta da intrusioni grazie a strumenti dedicati (firewall e antivirus). La rete, inoltre, è cablata e protetta. Firewall e antivirus sono attivi su tutte le postazioni.
Custodia supporti amovibili	
Applicata	Gli utenti possono utilizzare le memorie di massa USB per acquisire dati e sono responsabili della loro custodia. L'Azienda ha definito per il personale specifiche regole operative per la gestione dei supporti amovibili.
Distruzione dei dati residuali	
Applicata	Eventuali attività di dismissione di apparecchiature informatiche vengono affidate – secondo necessità – a società esterne che effettuano servizi di assistenza tecnica.
Misure di ripristino	
Applicata	A garanzia del ripristino dei dati l'Azienda esegue l'attività di backup per tutte le banche dati come sopra definito; per eventuali ripristini hardware l'azienda si è dotata di specifici contratti di manutenzione che prevedono tempi di intervento e risoluzione certi.
Conformità dai soggetti applicanti le misure standard	
Applicata	Gli interventi da parte dei fornitori terzi avvengono solo su richiesta o secondo necessità. A conclusione dell'intervento, viene rilasciato dal fornitore un verbale dell'intervento eseguito e delle misure adottate.
Istruzioni agli incaricati col fine di custodia e controllo degli archivi cartacei	

Applicata	Sono state impartite istruzioni agli incaricati finalizzate al controllo ed alla custodia degli atti e dei documenti contenenti dati personali.
Trattamenti non automatizzati – protezione dati	
Applicata	Vedi "Istruzioni agli incaricati col fine di custodia e controllo degli archivi cartacei"
Trattamenti non automatizzati – accesso fuori orario	
Applicata	Eventuali accessi fuori dagli orari di lavoro avvengono sono da parte di personale preventivamente autorizzato.

Oltre a quanto suddetto, sono implementate le misure minime di sicurezza ICT previste per la pubblica amministrazione come previsto dalla Circolare AgID n. 2/2017, i cui dettagli implementati sono descritti nel documento parte integrante del presente manuale denominato "MISURE MINIME DI SICUREZZA ICT PER LE PA vers. 1.0".

3.2 Dettaglio adeguamento alle misure di cui all'Art. 32 del RGPD

Con l'entrata in vigore del Regolamento europeo sulla privacy viene posta particolare attenzione alle modalità di trattamento e conservazione dei dati definiti "particolari" quindi sensibili, giudiziari o riferibili a soggetti minori (età inferiore a 16 anni).
Tali attenzioni variano in base all'ambito di operatività dell'azienda, alle modalità di trattamento e conservazione dei dati.

La Napoli Servizi tratta sicuramente dati "particolari" che utilizza per finalità di gestione del personale nonché per lo svolgimento di attività specifiche svolte per conto del Comune di Napoli. I dati di questi soggetti, oltre ad essere di tipo anagrafico possono riferirsi anche a condizioni fisiche particolari. Sebbene non tutti questi dati siano trattati a mezzo di strumenti elettronici, è necessario introdurre in azienda una maggiore consapevolezza tra il personale dipendente, circa i rischi legati a trattamenti di dati personali "particolari" non conformi alla norma e alle regole aziendali.

Per ognuno dei sistemi informatici, il Regolamento prescrive l'attuazione di misure tecniche ed organizzative finalizzate a minimizzare l'accesso abusivo ai dati, la manomissione e/o distruzione degli stessi, il furto delle informazioni.

Tra le misure tecnico organizzative previste dal legislatore europeo troviamo:

- Cifratura o pseudonimizzazione dei dati;
- Capacità di assicurare riservatezza, integrità e disponibilità;
- Ripristino tempestivo dei dati in caso di incidente fisico o tecnico;
- Test periodici per valutare con regolarità l'efficacia delle misure tecnico organizzative.

Inoltre, qualora si ravveda un evento di violazione dei suddetti dati personali, il Titolare deve avviare, entro il termine perentorio di 72 ore da quando ne è venuto a conoscenza, una notificazione alla Autorità

competente dando evidenza dell'accaduto. La comunicazione deve contenere informazioni con i dettagli tecnici dell'evento, i dati oggetto dell'eventuale violazione e i possibili impatti e conseguenze della violazione, le misure di sicurezza adottate per minimizzare il rischio. A tal proposito, è opportuno che il Titolare, con il supporto del Responsabile del settore IT, predisponga apposita procedura organizzativa (Data Breach) utile alla gestione di queste esigenze.

Napoli Servizi ha approntato una serie di misure specifiche per garantire la protezione dei propri sistemi informativi, con specifica attenzione alle banche dati contenenti categorie particolari di dati.
Una descrizione di dettaglio delle misure complessivamente poste in essere e delle misure che potrebbero essere ancora adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi è contenuta nel documento elaborato dalla Società per ottemperare a quanto previsto dalla Circolare AgID n.2/2017. Il documento in esame, come detto in precedenza, è parte integrante del presente Manuale e costituisce un importante strumento operativo e programmatico delle misure richieste per fornire un riferimento utile a stabilire il livello di protezione attualmente offerto dall'infrastruttura informatica di Napoli Servizi, nonché per individuare gli interventi idonei per il suo adeguamento.

4. Misure atte a garantire l'integrità e la disponibilità dei dati

Nel presente paragrafo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici;
- la sicurezza delle comunicazioni.

4.1 La protezione di aree e locali

Per quanto concerne il rischio d'area in generale, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da:

- gruppo di continuità dell'alimentazione elettrica;
- una assicurazione stipulata contro furto e incendio;
- armadi metallici.

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da:

- sistemi di autenticazione degli accessi negli uffici;
- presidio da parte di personale interno durante l'orario di apertura, dal servizio di vigilanza nelle ore di chiusura;
- accesso agli uffici delimitato dal suddetto presidio di vigilanza;
- armadi muniti di serratura dislocati nelle stanze;
- sistema di videosorveglianza.

In particolare, presso la sede di Napoli Servizi in Via G. Porzio isola C/1 è utilizzato un impianto di videosorveglianza con videoregistrazione. Ulteriori impianti di videosorveglianza presidiano anche le sedi operative di Via Piazzolla, parco De Filippo, piazza Telematica ed il magazzino di Via Imparato.
Le immagini rilevate dalla videosorveglianza sono salvate su hard-disk. Le finalità del trattamento sono riconducibili esclusivamente alla finalità di sicurezza e di tutela delle persone e del patrimonio.
L'impianto di videosorveglianza è costituito da telecamere poste nei corridoi degli uffici, che riprendono prevalentemente l'accesso agli uffici e alle uscite di sicurezza. I dati relativi alle immagini sono conservati temporaneamente per esclusive finalità di sicurezza e di tutela delle persone e del patrimonio.
Apposita cartellonistica, riportante gli elementi dell'art. 13 del RGPD, con particolare riguardo alle finalità e alla conservazione delle registrazioni, è stata collocata in prossimità delle telecamere e, comunque, in luoghi visibili a dipendenti e visitatori esterni.
Nell'adozione del sistema di videosorveglianza, Napoli Servizi ha provveduto a conformarsi alle disposizioni del RGPD e del Codice Privacy ed al Provvedimento Generale emanato da Garante per la protezione dei dati personali dell'8 aprile 2010.
L'installazione e l'esercizio delle apparecchiature è stata eseguita in ottemperanza e nel puntuale rispetto dei principi generali definiti dal Garante Privacy quali: principio di liceità, principio di necessità, principio di proporzionalità e principio di finalità.
In particolare, si precisa che:

- il sistema videosorveglianza viene utilizzato per la tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti o finalità di prevenzione di incendi o di sicurezza del lavoro;
- il sistema di videosorveglianza non effettua rilevazioni audio, per cui non sono possibili intercettazioni di comunicazioni o conversazioni;
- tutte le apparecchiature video facenti parti del sistema sono state installate e configurate in modo da escludere qualsiasi forma di controllo a distanza dei lavoratori o di aree non pertinenti;
- l'accesso allo storico delle immagini è possibile sono in presenza di opportune cautele e solo le autorità competenti sono legittimate ad accedere alle informazioni raccolte.

Inoltre, l'attività di videosorveglianza è esercitata osservando le seguenti indicazioni:

- sono fornite alle persone che possono essere riprese, indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
- sono raccolti i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando immagini dettagliate, ingrandite o con particolari non rilevanti;
- in nessun caso le telecamere sono posizionate in prossimità delle postazioni di lavoro;
- il periodo di conservazione dei dati è limitato allo stretto necessario e non eccede mai le 120 ore considerando la possibilità di consultare le registrazioni effettuate nei periodi di chiusura prolungata degli uffici (ponti, festività etc).

La conservazione dei dati oltre il termine previsto, è possibile solo in relazione al verificarsi di illeciti o quando siano in corso indagini giudiziarie.

I dati raccolti per fini determinati non sono utilizzati per finalità diverse o ulteriori, fatte salve le esigenze di polizia o di giustizia e non sono diffusi o comunicati a terzi.
Le registrazioni sono conservate sui dispositivi collocati nelle rispettive sedi in aree ad accesso ristretto.
L'accesso alle immagini in modalità live, così come l'accesso allo storico, è consentito esclusivamente ai soggetti espressamente autorizzati dall'azienda, con specifico incarico al trattamento delle immagini.

4.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, DVD, CD ROM, pen drive), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.
Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi ad un superiore, o ad un responsabile del trattamento, o direttamente al titolare.
Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.
In particolare, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

4.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato;
- realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative;
- realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus);
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (es. CD ROM, DVD, pen drive), nei quali siano contenuti dati personali.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza;
- dovere di elaborare in modo appropriato la parola chiave, che dovrà essere composte da almeno otto caratteri;
- dovere di conservare la segretezza sulla parola chiave, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema;

- obbligo di provvedere a modificare la parola chiave:
  - ✓ immediatamente, non appena viene consegnata loro da chi amministra il sistema;
  - ✓ successivamente, almeno ogni sei mesi per i dati personali. Tale termine scende a tre mesi, se la parola chiave dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari;
  - ✓ non riportando riferimenti agevolmente riconducibili all'interessato (nomi, cognomi, soprannomi, date di nascita proprie, dei figli o degli amici).

Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe rendersi necessario disporre delle parole chiave dell'incaricato, per accedere agli strumenti ed ai dati. In tal caso l'Amministratore di sistema, su autorizzazione del Titolare o del Responsabile del trattamento dei dati, provvede a "disabilitare" (fa scadere) la password di quell'incaricato e con una nuova password "accede" agli strumenti e ai dati, nel rispetto della privacy dell'incaricato, per tutte le operazioni necessarie o previste. Al termine dell'intervento l'Amministratore di sistema fa nuovamente scadere la password provvisoria. L'incaricato assente, al suo rientro, oltre ad esserne informato dovrà digitare una nuova password per accedere al suo PC.

L'accesso applicativo (profilo di autorizzazione) è diversificato per aree e competenze; periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

Per quanto riguarda la protezione di strumenti e dati da malfunzionamenti, attacchi informatici e programmi che contengono codici anomali (virus), sono stati presi in considerazione gli elementi sotto descritti.
In merito alla protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, la società è dotata di idonei strumenti elettronici e di programmi, in relazione al continuo evolversi dei virus, che sono sottoposti ad aggiornamento giornaliero.
In merito, invece, alla protezione degli elaboratori in rete dall'accesso abusivo, la protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall, nello specifico, per i casi in cui si trattino categorie particolari di dati o dati giudiziari.
Un terzo aspetto riguarda, infine, l'utilizzo di appositi programmi, la cui funzione è quella di prevenire la vulnerabilità degli strumenti elettronici, tramite la verifica di eventuali anomalie nella configurazione dei sistemi operativi e dei servizi di rete, correggendo di conseguenza i difetti insiti negli strumenti stessi.

Per quanto concerne i supporti rimovibili (es. CD ROM, DVD, pen drive), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano categorie particolari di dati o dati giudiziari.

Napoli Servizi ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti.

5. Criteri e modalità di ripristino dei dati

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

Per i dati trattati con strumenti elettronici, sono previste procedure per effettuare copie di sicurezza dei dati, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni.

Le copie vengono custodite presso le sedi o nel Cloud e in entrambi i casi in luoghi protetti.

6. Interventi formativi degli Incaricati

Per assicurare l'efficacia delle misure di sicurezza adottate dall' azienda è necessario che tutto il personale sia informato adeguatamente sulle stesse.

Per tale motivo è stato distribuito a tutto il personale il documento denominato "Regolamento informatico aziendale" – aggiornato periodicamente, secondo necessità - che individua i criteri operativi per il corretto utilizzo degli strumenti informatici, con particolare riferimento all'uso di Internet e della posta elettronica.

Inoltre, al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno le necessità di formazione del personale incaricato del trattamento dei dati, con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati.

6.1 Piano di Formazione del Personale autorizzato al trattamento dei dati

Sono stati effettuati e saranno predisposti nuovi interventi formativi finalizzati a rendere edotti **gli** incaricati del trattamento dei seguenti aspetti:

- l'uso del personal computer e della rete aziendale,
- i rischi che incombono sui dati,
- le misure disponibili adottate dall'azienda per prevenire eventi dannosi,
- i profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano,
- i comportamenti da assumere, in relazione ai compiti operativi assegnati,
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Gli interventi formativi sono programmati in modo tale, da avere luogo al verificarsi di una delle seguenti circostanze:

- al momento dell'ingresso in servizio, in caso di nuove assunzioni;
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del responsabile per la sicurezza o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.

7. Affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati all'esterno della struttura del Titolare si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza adeguate nel rispetto delle prescrizioni del RGPD.

Per la generalità dei casi, in cui il trattamento di dati personali, di qualsiasi natura, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto categorie particolari di dati o dati giudiziari, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali.

8. Controllo generale sullo stato della sicurezza

Al Responsabile del Settore Servizi Informativi è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze resi disponibili dalle nuove tecnologie, al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati e di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il Responsabile del Settore Servizi Informativi e gli altri incaricati del settore provvedono con frequenza almeno annuale, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici;
- verificare l'integrità dei dati e delle loro copie di back up;
- verificare la sicurezza delle trasmissioni in rete;
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti.

9. Dichiarazione d'impegno e firma

Il presente documento viene firmato in calce da:

- ✓ Amministratore Unico, in qualità di Titolare di NAPOLI SERVIZI S.P.A

Una sua copia verrà consegnata:

- ✓ al responsabile del trattamento dei dati;
- ✓ a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali.

Presa Visione:

Resp. Trattamento Dati
Mario Baggio

Resp. Protezione Dati
Angela Longobardi

Resp. della Transizione Digitale
Claudio Augusto

Il Titolare Trattamento Dati
Dott. Andrea de Giacomo