INFORMATIVA SUL TRATTAMENTO DEI DATI DEL PERSONALE DIPENDENTE

Si fornisce la presente informativa ai sensi degli art. 13 e 14 del Regolamento UE 2016/679 (di seguito: "Regolamento" o "GDPR") nonché delle norme del D. Lgs. n. 196/2013 ("Codice della Privacy"); lo scopo di questo documento è di informarLa, in particolare, su quali dei Suoi dati trattiamo, le finalità per cui li trattiamo e li condividiamo, per quanto tempo li conserviamo, quali sono i Suoi diritti e come potrà esercitarli.

*** * * * * * ***

1) Titolare del trattamento

Titolare del trattamento (di seguito: "Titolare") è il **Comune di Matera,** sede in Via Aldo Moro, 75100 Matera, rappresentato del sindaco Raffaello Giulio De Ruggeri, il Titolare potrà essere contattato al seguente indirizzo di posta elettronica

- *Contatti:* segreteria.sindaco@comune.mt.it

Questa amministrazione ha nominato *Responsabile Comunale della Protezione dei Dati Personali,* a cui gli interessati possono rivolgersi per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dalla normativa nazionale e comunitaria in materia di protezione dei dati personali:

- *Contatti:* wemapprivact@gmail.com

2) Finalità del trattamento

I Suoi dati sono trattati al fine dell'instaurazione, della gestione e dell'estinzione del rapporto di lavoro con il Titolare (quale dipendente, collaboratore, stagista, apprendista, etc.), nel pieno rispetto della disciplina applicabile; ossia per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa dell'Unione europea, da leggi, da regolamenti o da contratti individuali o collettivi, è finalizzato ad adempiere **obblighi previsti dalla legge nazionale sul contratto di lavoro alle dipendenze delle amministrazioni pubbliche** (d.lgs. 165/2001 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", d.lgs. 267/2000 "Testo unico delle leggi sull'ordinamento degli enti locali", d.P.R. 313/2002, artt. 28 e 32, "Testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti", d.P.R. 62/2013 "Regolamento recante codice di comportamento dei dipendenti pubblici"), nonché per il riconoscimento di agevolazioni ovvero l'erogazione di contributi, per l'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro o della popolazione, nonché in materia fiscale, sindacale, di tutela della salute, dell'ordine e della sicurezza pubblica.
In particolare, il trattamento è effettuato per

a) instaurare, gestire ed estinguere il Suo rapporto di lavoro ed ogni connesso aspetto contrattuale, previdenziale, assicurativo e fiscale;
b) la rilevazione delle presenze, la giustificazione delle assenze, il pagamento dei compensi, l'elaborazione delle buste paga, l'adempimento degli obblighi previdenziali e assistenziali, l'applicazione della normativa sulla sicurezza sui luoghi di lavoro, la formazione e quanto altro richiesto dalle normative di settore;

a) assolvere agli obblighi derivanti dalla normativa dell'Unione Europea, da norme di legge o da disposizioni cogenti (anche in materia di igiene e sicurezza del lavoro o della popolazione, tutela della salute, dell'ordine e della sicurezza pubblica, etc);
b) adempiere agli obblighi previsti in ambito fiscale e contabile;
c) adempiere agli obblighi previsti in ambito previdenziale ed assistenziale (anche integrativa);
d) assolvere agli obblighi derivanti dal Suo contratto individuale di lavoro e/o dalla contrattazione collettiva eventualmente a Lei applicabile (ivi inclusi gli adempimenti connessi al versamento di quote di iscrizione a sindacati o all'esercizio di diritti sindacale - quali ad es. gestione di permessi, distacchi, etc -, il riconoscimento di agevolazioni, l'erogazione di contributi, etc.);
e) la qualificazione e l'aggiornamento professionale dei dipendenti, nonché l'organizzazione di corsi di formazione;
f) adempiere ad ordini o provvedimenti dell'Autorità Giudiziaria, o di altre Autorità competenti;
g) far valere o difendere un diritto in sede giudiziaria, anche da parte di un terzo, alle condizioni previste dalla legge o dal "Regolamento";
h) rispondere a ogni Sua richiesta;
i) gestire le attrezzature dell'ente, anche informatiche, assegnateLe;
j) implementare ogni necessaria misura di sicurezza per prevenire il rischio di distruzione, perdita, diffusione, alterazione, furto, indisponibilità, accesso indebito e ogni altra attività non autorizzata avente a oggetto dati personali;
k) per finalità non direttamente attinenti all'adempimento di obblighi derivanti dal contratto di lavoro, ma che sono comunque riconducibili allo svolgimento dello stesso (indagini di clima, iniziative di comunicazione dell'ente, pubblicazione foto in riviste, sul portale intranet, sui canali web e "social" del "Titolare", stipula di convenzioni a favore dei lavoratori, etc.)
l) Eventuale ..... Gestire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio del datore di lavoro, anche rispetto, se relativi al profilo lavorativo cui ci si riferisce, al sistema di geolocalizzazione degli strumenti elettronici forniti per rendere la prestazione lavorativa ai sensi dell'art. 4, comma 3, l. 300/1970 (PC, smartphone, sistemi informativi, Internet, Posta elettronica).

3) Categorie di dati trattati

Il trattamento avrà come oggetto le seguenti categorie di dati personali

a) dati anagrafici (nome cognome, data e luogo di nascita, residenza, codice fiscale, etc.);
b) dati fiscali (Suoi e degli eventuali componenti del Suo nucleo familiare da Lei comunicati) ed estremi del conto corrente bancario.

Tali dati sono trattati per adempiere agli obblighi di legge o contrattuali (ad esempio, per l'elaborazione e la corresponsione della retribuzione, per il riconoscimento degli assegni familiari, etc.);

c) dati relativi allo stato di salute Suo o degli eventuali componenti del Suo nucleo familiare da Lei comunicati.

Anche tali dati saranno trattati per adempiere a specifici obblighi, anche previdenziali ed assistenziali, (malattie, infortuni, inabilità, etc.);

d) dati che si riferiscono al Suo rapporto di lavoro con il Titolare, come i riscontri sull'adempimento degli obblighi lavorativi (statistiche di presenza e assenza da lavoro), i dati per la gestione e

l’aggiornamento del Suo profilo professionale, di attribuzione di nuove mansioni e incarichi, di sviluppo professionale e di carriera, anche in forma di CV (eventualmente messo a disposizione dei clienti utilizzatori dei prodotti/servizi offerti dal Titolare ovvero per la partecipazione a eventi o convegni connessi alla propria attività lavorativa, anche all'estero), di valutazione delle prestazioni;

e) i dati relativi a eventuali iscrizioni sindacali e alla copertura di incarichi sindacali;
f) i dati relativi alla copertura di cariche pubbliche elettive al fine del godimento dei diritti previsti dalla legge;
g) i dati necessari al controllo delle spese dei dipendenti (pianificazione economica; predisposizione dei budget e della loro gestione; controllo delle voci di costo relative ai dipendenti; gestione delle spese di viaggio; gestione dei costi dei servizi telefonici, degli autoveicoli utilizzati, degli strumenti di office-automation in dotazione) nonché al fine di verificare - anche nel quadro di apposite azioni di auditing - la conformità degli adempimenti operativi alle normative e alle direttive istituzionali, l'adeguatezza del sistema di controllo dei processi amministrativi e la correttezza delle informazioni contabili e gestionali per adempiere agli obblighi di certificazione del bilancio;
h) i dati relativi all'utilizzo degli strumenti di lavoro, raccolti e trattati per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi (ad esempio, aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, back-up, etc.), per il controllo e la programmazione dei costi organizzativi (ad esempio, verifica costi di connessione a internet, traffico telefonico, etc.) ovvero per obblighi normativi;
i) i dati relativi agli accessi sul luogo di lavoro; in tale contesto potranno essere raccolti anche dati biometrici utilizzati per accrescere il livello di sicurezza nel controllo degli accessi a particolari ambiti sia dal punto di vista fisico - accessi ad aree di particolare interesse, che logico - accesso a sistemi particolarmente critici;
j) dati relativi alle immagini raccolti e trattati mediante sistemi di videosorveglianza destinati a garantire la sicurezza e la protezione e l'incolumità di beni e persone nel rispetto delle Sue prerogative e diritti, ove presenti nelle sedi nelle quali presta la sua attività.

Le immagini raccolte dai sistemi di videosorveglianza saranno trattate secondo i limiti e le modalità previsti della disciplina vigente, nonché sulla base delle indicazioni di cui Provvedimento dal Garante in data 8 aprile 2010 e, ove richiesti, degli accordi stipulati con le competenti organizzazioni sindacali o dell'autorizzazione rilasciata dalla DTL competente;

k) dati relativi a condanne penali o a reati.

Come sopra evidenziato, tra i dati oggetto di trattamento, potranno essere presenti anche dati “sensibili” (quelli che l’art. 9 del “GDPR” chiama << particolari >>), ossia quelli idonei, ad esempio, a rivelare l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale; ovvero i dati genetici, biometrici, relativi allo stato di salute (come infortuni, inabilità,etc), alla vita o all’orientamento sessuale, Suoi o di componenti del Suo nucleo familiare da Lei forniti; tali dati sono trattati nel rispetto delle disposizioni vigenti e dell’Autorizzazione Generale n. 1/2016 del 15/12/16 del Garante per la Protezione dei dati Personali (“Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro”).

Potranno inoltre essere oggetto di trattamento anche dati relativi a condanne penali e reati (di cui all’art. 10 del “GDPR”), tali dati saranno trattati nei limiti imposti dalla disciplina vigente.

4. Dati personali raccolti presso terzi

Potranno altresì essere trattati Suoi dati personali, raccolti presso terzi, per le medesime finalità già indicate.

Qualora ciò accadesse lo stesso avverrà nei limiti della disciplina vigente e Le verrà fornita, ove necessario, specifica informativa integrativa, in particolare circa le categorie dei dati raccolti presso terzi, la fonte da cui hanno origine detti dati nonché l'eventualità che i suddetti dati provengano da fonti accessibili al pubblico.

5. Base giuridica

I Suoi dati personali sono trattati per le finalità appena specificate, da parte della nostra Amministrazione, al solo fine di dare esecuzione al contratto di lavoro e/o adempiere agli obblighi di legge ai quali è soggetto il Titolare del trattamento.

Ai sensi dell'art. 6, paragrafo 1, lett. b), c), e) ed f) GDPR, i suddetti dati personali e particolari raccolti saranno trattati sulla base delle seguenti basi giuridiche:

- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6, lett. b);

- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, lett il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, lett. e);

- il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del Trattamento (art. 6, lett. f).

Con riferimento alle videoriprese o fotografie del dipendente, utilizzate per finalità di informazione, promozione delle attività dell'Amministrazione, didattica, partecipazione a progetti extra lavorativi, la base giuridica è rappresentata dal consenso dell'interessato ai sensi dell'art. 6, paragrafo 1, lett. a) del Regolamento.

Si specifica che i dati particolari possono essere trattati dal Titolare senza l'esplicito consenso dell'interessato, in quanto il loro trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale e nonché per finalità di medicina del lavoro e della valutazione della capacità lavorativa del dipendente (art. 9, par. 2, lettere b) e h) GDPR), o, infine, per consentire all'Amministrazione di accertare, esercitare o difendere un diritto in sede giudiziaria.

Potranno inoltre essere trattati dati personali a Lei riferiti, raccolti presso terzi, per le medesime finalità sopra indicate, nei limiti consentiti dalla legge applicabile e dal Regolamento.

Oltre a ciò, il Titolare del trattamento potrà trattare per finalità di sicurezza e controllo sui beni dell'amministrazione, le Sue immagini, eventualmente riprese dai sistemi di videosorveglianza, sulla base e secondo i limiti del provvedimento emanato dall'Autorità Garante per la protezione dei dati personali in data 8 aprile 2010, e successive modifiche, nonché degli accordi stipulati con le competenti organizzazioni sindacali o dell'autorizzazione rilasciata dalla ITL competente, laddove necessari.

Eventuale …….. L’Amministrazione potrebbe provvedere alla pubblicazione e/o diffusione in qualsiasi forma delle sue immagini/video sul sito internet, su carta stampata e/o qualsiasi altro mezzo di diffusione e alla conservazione delle foto stesse negli archivi, confermando che le finalità di tali pubblicazioni sono meramente di carattere pubblicitario e promozionale. Per tale particolare trattamento è richiesto il Suo consenso espresso.. c);

6. Comunicazione e diffusione

I Suoi dati personali potranno essere comunicati a terzi per assolvere gli obblighi stabiliti dalla legge o dal contratto (anche collettivo) applicabile, oltre che in esecuzione di eventuali deleghe da Lei conferite (ad esempio: accredito dello stipendio presso banche; versamento quote pensione integrativa, assicurazioni, cessione del quinto, etc.).

I Suoi dati personali potranno altresì essere comunicati a specifici soggetti individuati per la realizzazione di convenzioni in favore del personale dipendente, qualora sia stato prestato il consenso per le finalità di cui al precedente punto “2.”, co. 2, lett. “k)”.

I suoi dati potranno essere diffusi mediante affissione nelle bacheche situate nei posti di lavoro, ovvero con altre modalità in uso (intranet, app, etc.). nelle ipotesi tassativamente previste da norme di legge o di contratto (anche collettivo).

I dati potranno altresì essere messi a disposizione di società e/o professionisti che collaborano a vario titolo con il “Titolare”, ovvero a soggetti ai quali quest’ultimo affidi servizi in “outsourcing” (elaborazione delle buste paga; gestione degli adempimenti fiscali, previdenziali e assistenziali; conservazione e archiviazione dei dati personali dei dipendenti; installazione, sviluppo, cessazione e/o esercizio dei sistemi informativi ed informatici; revisione contabile; auditing, etc..

I dati potranno inoltre essere messi a disposizione di soggetti esterni all’organizzazione che forniscano servizi e/o prestazioni che siano comunque funzionali alle finalità indicate nella presente informativa (società che emettono “buoni pasto”; agenzie di viaggio in relazione a trasferte da Lei effettuate; società di noleggio auto; alberghi; etc.).

Tali soggetti, a seconda delle circostanze, tratteranno i Suoi dati in qualità di autonomi titolari o, quando necessario, quali responsabili del trattamento debitamente nominati da parte del Titolare.

I Suoi dati potranno, infine, essere messi a disposizione dell’Autorità Giudiziaria, o di altre Autorità competenti, ove a ciò tenuto il “Titolare”.

7. Trasferimento all'estero

I Suoi dati, nei limiti delle finalità indicate nella presente informativa, potranno essere trasferiti al di fuori dell’Unione Europea e dello Spazio Economico Europeo.

In tal caso detto trasferimento avverrà verso un Paese (od un settore specifico all’interno del detto Paese) od un’organizzazione internazionale che sia stato/a oggetto di una “Decisione di adeguatezza” della Commissione Europea ai sensi dell’art. 45 del “GDPR”.

In mancanza di “Decisioni di adeguatezza”, il “Titolare”, prima di trasferire i dati verso Paesi od organizzazioni internazionali terze, si premurerà di fornire garanzie adeguate nonché la sussistenza di obblighi di protezione e di sicurezza equivalenti a quelli garantiti dal Titolare medesimo, attraverso l'adozione di “norme vincolanti di impresa” o di “clausole tipo di protezione dei dati” adottate dalla Commissione Europea, ovvero attraverso l’utilizzo delle altre soluzioni indicate negli artt. da 44 a 49 del GDPR.

8. Modalità del trattamento

I dati personali potranno essere trattati sia mediante strumenti manuali e/o archivi cartacei e sia attraverso strumenti informatici (ivi compresi dispositivi portatili) e telematici, ma sempre sotto il presidio di misure tecniche e organizzative idonee a garantirne la sicurezza, l’integrità, la riservatezza e la disponibilità, ed evitare il loro uso illecito o non corretto.

I Suoi dati, anche qualora trattati da soggetti terzi (come i Responsabili del Trattamento) o da persone fisiche autorizzate al trattamento, saranno sempre trattati sulla base di specifiche istruzioni fornite dal “Titolare”, con particolare riferimento all'adozione e al rispetto delle misure di sicurezza, nonché atte a garantire l'assunzione da parte di tali soggetti di idonei obblighi di riservatezza in ordine ai dati personali trattati.

9. Tempi di conservazione

I Suoi dati personali verranno trattati dal “Titolare” per tutta la durata del Suo contratto di lavoro e, successivamente, per tutto il tempo in cui il Titolare è soggetto a obblighi di conservazione per finalità fiscali o per altre finalità previste dalla normativa dell’Unione Europea, da norme di legge o da disposizioni cogenti.

I Suoi dati personali, inoltre, potranno essere trattati, anche successivamente alla cessazione del Suo rapporto di lavoro con il “Titolare”, anche per il tempo necessario a far valere o tutelare i diritti di quest’ultimo o di altre società del Gruppo, ove necessario.

10. Processo decisionale automatizzato

Il Titolare, per il trattamento dei dati, non si avvale di un processo decisionale automatizzato.

10. Conseguenze della mancata comunicazione dei dati personali

Come sopra indicato, il conferimento dei Suoi dati è necessario per poter procedere all'instaurazione del rapporto di lavoro nonché per dare esecuzione a obblighi derivanti dalla normativa dell’Unione Europea, da norme di legge, da disposizioni cogenti o dal contratto (individuale e/o collettivo), e ciò anche in relazione ai Suoi dati di natura sensibile.

La mancata comunicazione dei Suoi dati personali, pertanto, impedirebbe l’effettuazione di alcune prestazioni (istituti contrattuali o garantiti dalla legge a tutela della maternità o dell'handicap, o in relazione a infortuni sul lavoro, etc.) e, in taluni casi, potrebbe addirittura rendere impossibile instaurare o proseguire il rapporto di lavoro.

In particolare, per le finalità di cui al punto “2.”, co. 2, lett. “k)”; il conferimento dei dati è facoltativo ed è richiesto il Suo consenso libero e informato che potrà revocare liberamente senza che vi siano conseguenze nel rapporto di lavoro, fermo restando che tale rifiuto potrebbe rendere impossibile l'erogazione di alcuni servizi a Suo favore o rendere meno efficaci alcune iniziative intraprese dal “Titolare”.

11. I Suoi Diritti

La normativa applicabile Le riconosce tutta una serie di diritti che Lei potrà esercitare in qualunque momento, tra cui quelli di:

- chiedere al titolare
  l'accesso ai Suoi dati personali ed alle informazioni relative agli stessi;
  la rettifica dei dati inesatti o l'integrazione di quelli incompleti;
  la cancellazione dei dati personali che La riguardano (al verificarsi di una delle condizioni indicate nell'art. 17, par. 1, del “GDPR” e nel rispetto delle eccezioni previste nel paragrafo 3 dello stesso articolo);
  la limitazione del trattamento dei Suoi dati personali (al ricorrere di una delle ipotesi indicate nell'art. 18, paragrafo 1 del GDPR);
- richiedere ed ottenere dal titolare - nelle ipotesi in cui la base giuridica del trattamento sia il contratto o il consenso, e lo stesso sia effettuato con mezzi automatizzati - i Suoi dati personali in un formato strutturato e leggibile da dispositivo automatico, anche al fine di comunicare tali dati ad un altro titolare del trattamento (“diritto alla portabilità dei dati personali”);
- opporsi in qualsiasi momento al trattamento dei Suoi dati personali al ricorrere di situazioni particolari che La riguardano;
- revocare il consenso in qualsiasi momento, limitatamente alle ipotesi in cui il trattamento sia basato sul Suo consenso per una o più specifiche finalità, fatto salvo l’interesse legittimo del Titolare. Il trattamento basato sul consenso ed effettuato antecedentemente alla revoca della stessa conserva, comunque, la sua liceità;
- il diritto di opporsi al trattamento dei dati personali basato sull'interesse legittimo del Titolare; in questo caso il Titolare non continuerà a processare i dati personali a meno che non sia in grado di dimostrare una base legittima per il trattamento che prevalga sui Suoi interessi ed i Suoi diritti, oppure per ragioni legali.
- proporre reclamo ad un'autorità di controllo (Autorità Garante per la protezione dei dati personali – www.garanteprivacy.it).

12. Data Protection Officer

Il Titolare ha provveduto a nominare il Data Protection Officer (Responsabile della Protezione dei Dati), ai sensi dell’art. 37 del “GDPR”, il quale potrà essere contattato al seguente indirizzo di posta certificata: wemapp@pec.it ovvero al seguente indirizzo di posta elettronica ordinaria: wemapprivacy@gmail.com

Copia della presente informativa sarà comunicata è consegnata a ciascun dipendente, collaboratore e stagista nel momento in cui si instaura il rapporto di lavoro, è pubblicata sulla intranet e è tenuta permanentemente affissa presso le bacheche di tutti i posti di lavoro.

Distinti saluti.

- Il Comune di Matera -

Per presa visione della presente informativa.

Matera, (data)

Firma

_____

Dichiarazione di consenso ai sensi dell'art. 7 del Regolamento UE 2016/679

Il/La sottoscritto/a _____, nato/a _____ il _____

preso atto della presente informativa, fornita ai sensi degli artt. 13 e 14 del GDPR, in ordine al trattamento dei propri dati personali ed alle conseguenze in ordine a un eventuale rifiuto,

( ) esprime ( ) **non** esprime

il proprio consenso al trattamento dei dati personali per le finalità di cui al punto punto “2.”, co. 2, lett. “l)” della stessa informativa.

Matera,

Firma

_____

Ad implementazione delle informazioni già rilasciate, il lavoratore deve altresì essere informato e attenersi alle seguenti modalità operative sul trattamento dei dati personali

MANUALE OPERATIVO PRIVACY

Organizzazione	**Comune di Matera**

SEDE	**Municipio** **Via Aldo Moro,** **75100 Matera - MT**

Rev 1
Data revisione: 17/05/2019

Indice delle revisioni

N.REV.	DATA REV.	DESCRIZIONE
00	18/05/2019	Emissione

1. DEFINIZIONI

General Data Protection Regulation (GDPR)
Il Regolamento generale per la protezione dei dati personali n. 2016/679 è la normativa europea in materia di protezione dei dati personali di persone fisiche. Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016 ma la sua attuazione è avvenuta a distanza di due anni, a partire dal 25 maggio 2018.
Trattandosi di un regolamento non necessita di recepimento da parte degli Stati dell'Unione per cui è attuato allo stesso modo in tutti gli Stati dell'Unione. Il suo scopo è, infatti, la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea.

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

Dato personale
Qualsiasi informazione concernente una persona fisica identificata o identificabile (art. 4 GDPR), anche indirettamente, oppure informazioni (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari.

Dati particolari
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.

Profilazione
Per profilazione si intende l'insieme delle attività di raccolta ed elaborazione dei dati inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento. In ambito commerciale, la profilazione dell'utente è il mezzo che consente la fornitura di servizi personalizzati oppure l'invio di pubblicità comportamentale.

Pubblicità comportamentale
La pubblicità comportamentale è una tecnica basata sul tracciamento (tracking) delle attività online degli utenti, al fine di costruire dei profili degli utenti con lo scopo di offrire loro pubblicità più rilevante per gli utenti stessi, e quindi più efficace.

Titolare
Il Titolare del trattamento (data controller) è "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. par. 1, n. 7 GDPR).

Responsabile del trattamento
Il responsabile del trattamento è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare (art. 4, par. 1, n. 8 GDPR).

Sub responsabile
Il responsabile del trattamento può nominare responsabili di secondo livello a meno che non sia vietato dalle istruzioni del titolare. È comunque il responsabile principale a rispondere di fronte al titolare del trattamento dell'operato dei sub-responsabili. Al sub-responsabile devono essere fornite le istruzioni e deve operare nel rispetto degli obblighi imposti al responsabile del trattamento.

Persona autorizzata
Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato
La persona fisica a cui si riferiscono i dati personali.

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

Misure di sicurezza
Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che assicurano un livello di protezione adeguato dei dati personali.

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

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

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

Parola chiave
Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

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

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

2. RUOLI, COMPITI E NOMINA DEI SOGGETTI

2.1 Titolare del Trattamento

Il **Titolare del trattamento è** 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.
Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

Il Titolare mette in atto le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR, le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

2.2 Responsabile del Trattamento dati

2.2.1 Compiti delle persone autorizzate al trattamento dei dati personali

Il responsabile del trattamento (data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR).
Si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.
Il titolare del trattamento risponde della gestione effettuata dal responsabile, dovendo ricorrere a responsabili che presentino garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che soddisfino i requisiti del Regolamento (Considerando 81 GDPR), e che le sue decisioni siano conformi alle leggi. Compito specifico del titolare è, infatti, quello di valutare il rischio del trattamento che pone in essere tramite i responsabili. Il titolare deve sempre poter sindacare le decisioni dei responsabili.
Il responsabile ha obblighi di trasparenza, occorre, infatti contrattualizzare il rapporto tra titolare e responsabile specificando gli obblighi ed i limiti del trattamento dati. Il responsabile riceverà, tramite atto giuridico (cioè per iscritto), tutte le istruzioni in merito ai trattamenti operati per conto del titolare, alle quali dovrà attenersi. Inoltre il responsabile del trattamento dovrà mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento, e dovrà tenere il registro dei trattamenti svolti (ex art. 30, paragrafo 2, GDPR).
Il responsabile ha, poi, l'obbligo di garantire la sicurezza dei dati adottando tutte le misure di sicurezza adeguate al rischio (art. 32 GDPR), tra le quali anche le misure di attuazione dei principi di privacy by design e by default, garantendo la riservatezza dei dati, vincolando i dipendenti, informando il titolare delle violazioni avvenute ed occupandosi della cancellazione dei dati alla fine del trattamento.

Gli accordi, che possono avere solo la forma scritta e con atto vincolante per il responsabile del trattamento, dovrebbero prevedere: l'obbligo di trattare i dati solo in conformità alle istruzioni ricevute dal titolare; l'obbligo di garantire che le persone fisiche autorizzate alle attività di trattamento siano vincolate da obblighi di riservatezza, contrattualmente assunti o stabiliti per legge; l'obbligo di adottare le misure richieste ai sensi dell'art. 32 del Regolamento, vale a dire le misure tecniche e organizzative a protezione dei dati ritenuti idonee a garantire un livello di sicurezza adeguato al rischio insito nel trattamento; l'imposizione degli stessi obblighi verso l'eventuale sub-responsabile; l'obbligo di assistere il titolare, mediante misure tecniche e organizzative adeguate, e nella misura in cui ciò sia possibile, nel dar seguito alle eventuali richieste degli interessati (accesso, rettifica, cancellazione, portabilità, opposizione); le attività di notificare di eventuali data breach.

2.2.2 Nomina del Responsabile del trattamento dei dati personali

La nomina di ciascun Responsabile del trattamento dei dati personali deve essere effettuata dal Titolare del trattamento con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

2.3 Persona autorizzata al trattamento dei dati personali

2.3.1 Compiti delle persone autorizzate al trattamento dei dati personali

Gli **Autorizzati del trattamento** sono le persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali dal **Responsabile del trattamento**.

In particolare, gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

A tal fine, vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal titolare/responsabile;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
    - divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del titolare/responsabile;
    - l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
    - per ogni trattamento dei dati personali deve essere sempre utilizzata l'idonea base giuridica che legittima il trattamento secondo quanto stabilito dagli art. 6, 9 e 10 del Regolamento UE 679/2016;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;

- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

2.3.2 Designazione delle persone autorizzate al trattamento dei dati personali

La designazione di ciascuna **Persona autorizzata al trattamento dei dati personali secondo l'art 2**-*quaterdecies del d.lgs 196/2003* deve essere effettuata dal **Titolare** o dal **Responsabile del trattamento** con una **lettera di incarico** in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.

3. ATTIVITÀ DI TRATTAMENTO DATI PERSONALI

Ogni dipendente deve conoscere il registro delle attività di trattamento approvato dall'organizzazione. Il Registro riporta almeno le seguenti informazioni:

- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
  - categorie di dati personali;
  - categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
  - ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

VALUTAZIONE DEI RISCHI – METODOLOGIA UTILIZZATA
Per ogni attività di trattamento è stata eseguita la valutazione dei possibili scenari di rischio.
Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	**Improbabile**
2	**Poco probabile**
3	**Probabile**
4	**M. Probabile**
5	**Quasi certo**

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ LR ≤ 3)*
Medio - basso	*(4 ≤ LR ≤ 6)*
Rilevante	*(8 ≤ LR ≤ 12)*
Alto	*(15 ≤ LR ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

4. ASSET AZIENDALI

Gli asset sono tutti gli strumenti utilizzati dall'organizzazione per trattare e conservare i dati personali quali:

- server, computer, tablet, smartphone, sistemi di rilevazione presenze;
- programmi software sia installati su dispositivi aziendali che utilizzati in cloud;
- archivi relativi a database, cartelle condivise, ecc.

5. ISTRUZIONI OPERATIVE AUTORIZZATI DEL TRATTAMENTO

Codice:	PR05
Revisione:	00
Data della revisione:	18/05/2019

INDICE

- Prescrizioni per gli autorizzati

- Addetti alla manutenzione
- Osservanza delle disposizioni in materia di Privacy.
- Non osservanza della normativa aziendale.
- Aggiornamento e revisione

PREMESSA

Il presente documento contiene le istruzioni operative per gli autorizzati del trattamento dei dati personali impartite dal Comune di Matera in qualità di titolare del trattamento, conformemente al Regolamento (Ue) 2016/679 (GDPR) ed alla normativa nazionale in vigore. I dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso di questa Organizzazione diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che, anche inconsapevolmente, potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'organizzazione.

DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e la normativa nazionale in vigore, si definisce:

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

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

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.

ADEMPIMENTI

Ciascun autorizzato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- **rispettare l'obbligo di riservatezza e segretezza** e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto se non previsto da una espressa base giuridica;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- **rispettare le misure di sicurezza** idonee adottate dall'organizzazione, atte a salvaguardare la riservatezza e l'integrità dei dati;
- **segnalare anche per iscritto eventuali malfunzionamenti** di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- **accedere ai dati strettamente necessari** all'esercizio delle proprie funzioni e competenze;
- in caso di **interruzione del lavoro**, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- **mantenere riservate le proprie credenziali di autenticazione**;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.
- **Partecipare costantemente alle Formazione** proposta dall'ente in materia alla privacy e alla protezione dati personali
- **Autovalutarsi** con attenzione, mediante modelli di questionari predisposti o mediante altre modalità da concordare con il data protection officer dell'organizzazione;
- garantire che la(e) finalità si conformi(no) alla legge applicabile e si fondi(no) su una base legale ammissibile;
- **comunicare all'interessato la(e) finalità prima del momento** in cui le informazioni sono raccolte o utilizzate per la prima volta per una nuova finalità;
- **se del caso, fornire spiegazioni sufficienti dell'esigenza di trattare dati sensibili**.
- **notificare violazioni della privacy ai responsabili** definiti nelle procedure

dell'organizzazione non appena si venga a conoscenza di una vulnerabilità e di un rischio per gli individui

- **Alla cessazione dell'attività lavorativa non utilizzare le autorizzazioni** ancora in essere e comunicare ai responsabili le eventuali de-registrazioni da effettuare.
- Nel caso di variazioni di responsabilità o impiego è necessario informare tempestivamente i responsabili se ci si rende conto che le credenziali di accesso sono ancora attive.
- assicurare che gli asset di cui si è responsabile siano inventariati
- assicurare che gli asset siano appropriatamente classificati e protetti
- Classificare asset e informazioni in base al regolamento dell'organizzazione
- definire, relativamente ai propri asset, appropriate regole di controllo di accesso, diritti di accesso e limitazioni per i ruoli specifici degli utenti, con un livello di dettaglio e una severità di controllo proporzionali al rischio relativo alla sicurezza delle informazioni.

MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli autorizzati del trattamento sono:

identificazione dell'interessato: al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

verifica del controllo dell'esattezza del dato e della corretta digitazione: al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

Norme logistiche per l'accesso fisico ai locali: I locali ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto, le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

Limitazione della raccolta: limitare la raccolta dei dati personali a quanto rientra nei limiti della legge applicabile ed è strettamente necessario per la(e) finalità specificata(e)

Minimizzazione dei dati: ridurre strettamente al minimo il trattamento di dati personali. Minimizzare i dati personali che sono trattati e il numero dei privacy stakeholder e delle persone alle quali i dati personali sono divulgati o che hanno accesso ad essi; assicurare l'adozione di un principio di "necessità, per cui ciascuno dovrebbe avere accesso soltanto ai dati personali necessari per lo svolgimento delle proprie mansioni ufficiali nel quadro della finalità legittima del trattamento di dati personali. L'Ente deve applicare l'anonimizzazione o la pseudonimizzazione ai dati personali, se possibile, per ridurre il rischio per gli interessati.

Rilevazione presenze: Ove possibile, si raccomanda di dotare le sedi dell'Organizzazione di un servizio di un servizio di reception / sorveglianza. In questo caso, ogni autorizzato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

Misure organizzative per favorire l'esercizio dei diritti degli interessati: Attuare con attenzione Misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità' e la completezza del riscontro fornito agli interessati

ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).

È obbligatorio mantenere una separazione dell'uso privato e per l'attività istituzionale o di business dei dispositivi, fino ad utilizzare del software per supportare questa separazione e per proteggere i dati su un dispositivo privato;

Se si utilizzano strumenti privati a fornitura dell'accesso alle informazioni sono dopo che gli utenti hanno sottoscritto un accordo per l'utente finale riconoscendo i loro obblighi (protezione fisica, aggiornamento del software ecc.) rinunciando alla proprietà dei dati e permettendo la cancellazione remota dei dati da parte dell'organizzazione in caso di furto o smarrimento del dispositivo o quando non più autorizzati a utilizzare il servizio.

Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

Gestione strumenti elettronici (pc fissi e portatili)

Ciascun autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza,

consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.

Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

• al **termine delle ore di servizio, il PC deve essere spento**, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;

• **Se l'autorizzato si assenta momentaneamente dalla propria postazione** deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto, deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;

• **Relativamente all'utilizzo dello screen-saver**, occorre osservare le seguenti norme:

- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
- Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

• Quando si esegue la **stampa di un documento** contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento, **conviene prediligere le stampanti che hanno un pin per attivazione della stampa;**

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

• prima della riconsegna, rimuovere eventuali file ivi elaborati;

• quando il PC portatile è nei locali dell'organizzazione, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando appositi cavi in acciaio dotati di lucchetto;

• quando il PC portatile è all'esterno dell'organizzazione, evitare di lasciarlo incustodito;

• per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;

• in caso di **furto di un portatile** è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi;

• in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;

• **eseguire periodicamente salvataggi dei dati e non tenere tali backup** insieme al PC portatile. Per i backup è necessario attenersi alla politica sui backup di questa organizzazione.

Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Autorizzato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

• tutela l'utilizzatore ed in generale l'organizzazione da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;

• tutela l'Autorizzato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;

• è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun autorizzato deve scegliere le password in base ai seguenti criteri:

- **devono essere lunghe** almeno otto caratteri nel caso di **password**;
- **devono essere lunghe** non meno di 20/30 caratteri in caso di **passphrase**;
- non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
- le password devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
- le passphrase devono contenere almeno un numero e uno dei segni speciali, lettere, maiuscole e minuscole
- non deve essere uguali alle precedenti.

Per la **corretta gestione della password** è necessario:

- Almeno ogni **3 mesi è obbligatorio cambiare la password**;
- **Ogni password ricevuta va modificata al primo utilizzo**;
- La **password venga conservata in un luogo sicuro**;
- **Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono**;
- **Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni**.
- Le credenziali sono disattivate in caso di perdita della qualità

- Le credenziali sono disattivate se inutilizzate per sei mesi

Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici. Pertanto, si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

- **Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati**;
- **Non installare sistemi per connessione esterne** (es: modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- **Non installare programmi, anche in versione demo**. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
- **Non modificare i parametri di configurazione del proprio PC** senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

Gestione posta elettronica

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'organizzazione e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza dell'organizzazione e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

- Se si ricevono **mail da destinatari sconosciuti e ritenuti inaffidabili contenenti file di qualsiasi tipo**, procedere alla loro immediata eliminazione;
- È **fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali** o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- **La casella di posta elettronica assegnata deve essere mantenuta in ordine**, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Nell'ipotesi in cui la e-mail debba essere utilizzata per la **trasmissione di dati particolari (ex dati sensibili),** si raccomanda di prestare attenzione a che:

- **l'indirizzo del destinatario sia stato correttamente digitato**,
- **l'oggetto del messaggio** non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- **nel corpo del messaggio** sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;
- **Nel caso in cui si debbano trasmettere documenti contenenti dati sensibili si deve valutare con attenzione la criptazione degli allegati da trasmettere per esempio con pdf criptati mediante passwor**d

Gestione del salvataggio dei dati

Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Autorizzato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…). L'Autorizzato deve verificare che i supporti informatici utilizzati per il backup siano funzionali e non corrotti**. Il backup deve essere eseguito mediante software sul cloud con criptazione pear to pear, backup giornaliero e data retention** almeno per 120 giorni oppure con dischi magnetici esterni, CD e DVD.

Prevenire il rischio del deperimento dei supporti durante il periodo in cui i dati archiviati sono ancora necessari mediante il trasferimento dei dati su supporti nuovi prima che diventino illeggibili;

Gestione dei supporti rimovibili

Si *sconsiglia* **l'uso dei supporti rimovibili come le penne usb e gli hard disk esterni**. Se proprio necessario il loro utilizzo deve essere autorizzato dal centro elaborazione dati**. In tutti i casi non possono essere utilizzati per memorizzare dati sensibili o dati giudiziari a meno che questi non siano crittografati.**

Inoltre, questi dispositivi, diversi dalla firma digitale, devono essere monitorati con costanza e devono essere utilizzati sempre negli stessi pc.

Non è consentito lo scambio di dati mediante chiavette usb e hard disk esterni provenienti da soggetti esterni all'organizzazione.

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati

devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del Centro Elaborazione Dati. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili) /giudiziari devono essere crittografati.

Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Azienda è stato installato un software antivirus che si aggiorna automaticamente all'ultima versione disponibile.

L'antivirus non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.

Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso. Ogni autorizzato è responsabile degli asset a lui assegnati.

6. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Codice:	PR06
Revisione:	00
Data della revisione:	18/05/2019

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi**. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi**. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.

Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure **l'abbandono in vista sulle scrivanie** quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

- **distruzione delle copie cartacee**

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, **sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta**, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

- **Misure di sicurezza**

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Autorizzato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Autorizzato stesso. In particolare, si richiede:

- la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
- la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di una trita documenti.

- **Prescrizioni per gli autorizzati**

L'Autorizzato deve attenersi alle seguenti prescrizioni:

- in **nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro** strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- **la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli autorizzati, deve comunque essere rimossa al termine dell'orario di lavoro**;
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
- **i supporti devono essere archiviati in ambiente ad accesso controllato**;
- i documenti contenenti dati personali non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
- **il numero di copie** di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- **cassetti ed armadi contenenti documentazione riservata debbono**

tassativamente essere chiusi a chiave fuori dell'orario di lavoro;

- l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Autorizzato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
- **la distruzione** di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Autorizzato;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Autorizzato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli autorizzati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli autorizzati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- **l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato**. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. **Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate**.
- è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.
- **Ogni dipendente deve conoscere la politica per l'accesso di questa organizzazione**

ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:

- Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
- **gestire le credenziali di autenticazione dei soggetti autorizzati del trattamento su indicazione dell'Amministratore di sistema**;
- gestire i profili di autorizzazione degli autorizzati al trattamento dei dati, su specifiche impartite dai responsabili di funzione, su indicazione dell'Amministratore di sistema;
- **provvedere alla disattivazione/variazione delle utenze**, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione

dell'Amministratore di sistema;

- **custodire la documentazione cartacea,** prodotta nello svolgimento dei propri compiti istituzionali;
- **L'accesso agli addetti alla gestione e manutenzione è consentito** unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
- **A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione,** è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:
- **Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.**
- Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
- **Per effettuare operazioni di manutenzione sui database che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.**
- Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
- È necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
- Tutti i dati personali contenuti nei data base devono essere protetti da password;
- **Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli autorizzati, attenersi alle seguenti indicazioni**:
    - **in presenza** dell'autorizzato, **far digitare la password dall'autorizzato** stesso evitando di venirne a conoscenza;
    - **in assenza** dell'autorizzato rivolgersi alla persona individuata dall'autorizzato quale proprio fiduciario il quale provvederà all'inserimento della password.
- Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
- L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;
- **Qualora si renda necessario prelevare apparecchiature elettroniche** per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'autorizzato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
- l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di

password e ID;

- **È assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dall'organizzazione, se non previa espressa comunicazione scritta;**
- N**el caso in cui ci si avvalga di soggetti esterni (sub-responsabili)** per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

Trasporto di supporti fisici

Dovrebbero essere considerate le seguenti linee guida per proteggere i supporti che contengono informazioni e che devono essere trasportati:

- dovrebbe essere utilizzato un sistema di trasporto o un corriere affidabile;
- dovrebbe essere concordata con la direzione una lista dei corrieri autorizzati;
- dovrebbero essere sviluppate delle procedure per verificare l'identificazione dei corrieri;
- gli imballaggi dovrebbero essere adatti a proteggere il loro contenuto da danneggiamenti fisici che possono accadere durante il trasporto, in conformità con le specifiche del produttore, per esempio proteggendoli contro ogni fattore ambientale che può ridurre l'affidabilità dei supporti come l'esposizione al caldo, all'umidità o ai campi elettromagnetici;
- dovrebbe essere tenuto un registro che identifichi il contenuto dei supporti, la protezione applicata cosi come una traccia dei tempi del trasferimento ai custodi del transito e di ricezione a destinazione.

7 ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

Codice:	PR07
Revisione:	00
Data della revisione:	18/05/2019

INDICE

PREMESSA

Lo scopo di questo documento è quello di definire regole per l'utilizzo del sistema di informazione e di altre risorse di informazioni.

L'utilizzo delle risorse informatiche e telematiche della nostra organizzazione deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Comune di Matera ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

1. UTILIZZO DEL PERSONAL COMPUTER

Uso accettabile

Le risorse informative possono essere utilizzate solo per esigenze legate allo scopo di eseguire attività correlate all'organizzazione.

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'autorizzato con la massima diligenza e non divulgata.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna**.**

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa organizzazione, titolare del trattamento, di accedere ai dati trattati da ogni autorizzato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'autorizzato, informando tempestivamente l'autorizzato dell'intervento di accesso realizzato.

Attività proibite

Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Responsabile dei sistemi informatici*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici* **di Comune di Matera.** L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici*.

Non è consentito utilizzare applicazioni Java, controlli Active X e altri codici mobili, tranne quando autorizzati

Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete

può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici*.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici* nel caso in cui vengano rilevati virus.

La connessione alla rete dell'organizzazione da fuori deve avvenire esclusivamente mediante connessioni criptate (VPN)

2. UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

Il *Responsabile dei sistemi informatici* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli autorizzati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla **duplicazione dei dati**. È infatti assolutamente da evitare un'archiviazione ridondante.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

Il *Responsabile dei sistemi informatici* deve stipulare un contratto con una società terza, scelta in base alle proprie competenze professionali, per una valutazione periodica della sicurezza delle 'applicazioni web' e delle reti informatiche, di conseguenza i test riguarderanno tutto il sistema informatico. Ad esempio, l'analisi di un portale web inizia testando le diverse funzionalità, per poi concentrarsi sul meccanismo di autenticazione e

l'interazione con i database. Segue l'analisi della configurazione del relativo server e tutti gli elementi che lo circondano nella rete, e quindi tutti i dati e le informazioni di proprietà di una organizzazione (PenTest);

3. GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal ***Responsabile dei sistemi informatici.***

È necessario procedere alla modifica della password a cura dell'autorizzato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici. (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al Responsabile; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'autorizzato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*

La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici*, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Responsabile dei sistemi informatici*.

Quando le password sono usate come informazioni segrete di autenticazione, selezionare password di qualità con lunghezza minima sufficiente, che siano:

- facili da ricordare
- non basate su qualcosa che qualcun altro possa facilmente indovinare od ottenere utilizzando informazioni relative alla persona, per esempio nomi, numeri di telefono e date di nascita, ecc.;
- non vulnerabili ad attacchi a dizionario (ossia non composte da parole incluse nei dizionari)
- prive di caratteri consecutivi identici, formate da soli caratteri alfanumerici o numerici
- se temporanee, cambiate al primo log-on;

Non usare le stesse informazioni segrete di autenticazione per scopi istituzionali/aziendali e non.

Tener conto sempre della seguente politica delle password:

- forzare l'uso di identificativi utente e password individuali per mantenere la tracciabilità;
- permettere agli utenti di selezionare e cambiare la propria password e includere una procedura di conferma per errori di input;
- forzare la scelta di password di qualità;
- forzare gli utenti a cambiare la loro password al primo log-on;
- forzare un cambio periodico e quando necessario delle password;
- mantenere una registrazione delle password precedentemente usate per prevenire il loro riuso;
- non mostrare le password sullo schermo quando vengono inserite;
- memorizzare i file delle password separatamente dai dati del sistema applicativo;
- memorizzare e trasmettere le password in modo protetto.

4. UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

5. UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

6. USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'organizzazione a Voi, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica dell'organizzazione per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Comune di Matera deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'organizzazione "know how" tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'organizzazione, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).

Per la trasmissione di file all'interno di Comune di Matera è sconsigliabile utilizzare la posta elettronica anche se possibile, prestando attenzione alla dimensione degli allegati. È conveniente utilizzare strumenti di condivisione concordati con il *Responsabile dei sistemi informatici*.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile dei sistemi informatici*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

7. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa**. È assolutamente** *proibita* **la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa**.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici*.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

È necessario inoltre:

- **chiudere le sessioni attive** quando hanno completato l'attività, a meno che non possano essere protette da un appropriato meccanismo di bloccaggio, per esempio screen saver protetto da password;
- **effettuare il log-off da applicazioni o servizi di rete quando non più necessari**;
- **proteggere il computer o i dispositivi mobili, quando non in uso, da un utilizzo non autorizzato con una chiusura a chiave o con un controllo equivalente, per esempio una password di accesso.**

8. BEST PRACTIES DA SEGUIRE

Esaminare quali informazioni sono disponibili nella propria organizzazione per determinare se tutte le informazioni personali sono state raccolte per scopi specifici e se è ancora necessario conservare queste informazioni.

Conservare le informazioni personali solo nei luoghi individuati o comunque inventariare sempre un nuovo archivio informatico o cartaceo.

Effettuare verifiche periodiche o controlli a campione per garantire che le informazioni personali vengano conservate con misure di sicurezza idonee al trattamento, alla probabilità di rischio, al tipo di informazioni contenute, alla sensibilità delle informazioni personali, la quantità e i tipi di informazioni detenute, come vengono trasmessi e a quante persone, in quali formati;

Per evitare divulgazioni improprie, stabilire metodi sicuri per distruggere le informazioni non più necessarie (ad esempio, distruggere file cartacei o eliminare in modo sicuro i record elettronici). Considerare, ad esempio, i **rischi associati allo smaltimento di computer o stampanti** in cui le informazioni personali sono state lasciate sul disco rigido.

Obbligare mediante contratti sottoscritti con atti vincolanti i responsabili esterni a conservare i dati solo per il periodo necessario e comunque a rispettare le norme vigenti in tema di protezione dati personali;

Non condividere mai le informazioni personali con alcun individuo o sito Web a meno che la divulgazione sia prevista per norma e per regolamento.

Se il software di sicurezza del computer visualizza un avviso di sicurezza, prestare attenzione e chiamare l'amministratore di sistema.

Non collegare le unità USB al computer a meno che non si sappia da dove proviene, dove è stata collegata in precedenza e solo se strettamente necessario.

Utilizzare le e-mail e gli indirizzi e-mail in maniera idonea.

Per evitare le truffe via e-mail, tenere sempre presente l'indirizzo e-mail da cui viene inviata l'e-mail

Ogni applicazione web prodotta e utilizzata per i servizi di questo ente e richiede dati personali, deve utilizzare il protocollo "https:" e richiederlo nella barra di navigazione.

Conservare i dati personali cartacei in schedari o armadi chiusi a chiave dove l'accesso è consentito solo alle persone autorizzate;

Clean-desk: la necessità di non lasciare, soprattutto a fine giornata lavorativa, documenti contenenti dati personali e particolare sulla scrivania o comunque alla vista di altre persone non autorizzate.

Ogni autorizzato deve conoscere la politica di "scrivania pulita" per documenti ed i supporti di memorizzazione rimovibili, sia una politica di "schermo pulito" per i servizi di elaborazione delle informazioni di questa organizzazione.

Le politiche di scrivania pulita e di "schermo pulito" dovrebbero tenere in considerazione la classificazione delle informazioni (vedere punto 8.2), requisiti cogenti e contrattuali (vedere punto 18.1) nonché i corrispondenti rischi e gli aspetti culturali dell'organizzazione. Le seguenti linee guida dovrebbero essere considerate:

- le informazioni di business critiche, per esempio su carta o su supporti di memorizzazione digitale, quando non utilizzate, dovrebbero essere chiuse a chiave (idealmente in cassaforte o armadio o altri mobili con caratteristiche di sicurezza) soprattutto quando l'ufficio è vuoto;
- non si dovrebbero lasciare collegati computer e terminali o questi dovrebbero essere protetti, quando incustoditi, con un salva-schermo e meccanismi di blocco della tastiera controllati con una password o token o con altri meccanismi similari di autenticazione dell'utente e dovrebbero essere protetti da lucchetti con chiave, password od altri controlli quando non in uso;
- dovrebbe essere impedito l'uso di fotocopiatrici e di altre tecnologie di

riproduzione (per esempio scanner, fotocamere digitali);

- le stampe contenenti informazioni riservate o classificate dovrebbero essere rimosse immediatamente dalle stampanti.
- Una politica della scrivania/dello schermo pulito riduce i rischi di accesso non autorizzato, di perdita e di danneggiamento delle informazioni durante e al di fuori del normale orario di lavoro. Le casseforti o altre forme di archiviazione sicura potrebbero anche proteggere le informazioni da disastri quali incendi, terremoti, alluvioni o esplosioni.
- E da prendere in considerazione l'uso di stampanti con codice PIN, cosi che solo chi ha inviato il documento in stampa possa ritirarlo e solo quando si trovi in prossimità della stampante.

Accesso limitato alle informazioni personali e ai luoghi di lavoro solo alle persone autorizzate o su sorveglianza.

Garantire che le protezioni fisiche e hardware siano sufficienti a proteggere da perdita o furto e da accesso, divulgazione, copia, utilizzo e modifica non autorizzati.

Garantire la responsabilità della sicurezza dei dati: I vari tipi di dati personali dovrebbero essere classificati in modo che sia i lavoratori che i dirigenti capiscano le differenze. Classificando i dati personali, i dipendenti dovrebbero essere a conoscenza di come gestire ciascun tipo e quali tipi sono autorizzati a condividere o diffondere.

Applicare policy ai servizi web e di rete: stabilisce come si dovrebbero gestire problemi come l'accesso remoto e la gestione e la configurazione degli indirizzi IP e le politiche di rilevamento delle intrusioni.

Scansione per le vulnerabilità: È importante trovare eventuali vulnerabilità nell'infrastruttura IT prima degli hacker. Poiché gli hacker analizzeranno le vulnerabilità nel momento stesso in cui vengono scoperte, si dovrebbe avere una routine per controllare regolarmente le proprie reti.

Gestione delle patch: aggiornamenti continui dei sistemi software di base e non.

Criteri di sicurezza dei dati: Avere politiche condivise di gestione e protezione dei firewall, database e antivirus. Configurazione di server e sistemi operativi.

La risposta agli incidenti - Se si verifica una violazione della sicurezza, è importante disporre di misure appropriate per gestirla immediatamente. Ciò include la valutazione e la segnalazione dell'incidente e il modo in cui risolvere i problemi che ne derivano per evitare il ripetersi del problema.

Utilizzo accettabile: I dipendenti dovrebbero avere una politica di utilizzo corretto dei dati e dei sistemi ed è buona prassi fare firmare una politica di utilizzo.

Monitoraggio della conformità: attivare audit interni ed esterni servono a garantire che l'azienda rispetti i vari elementi di politica di sicurezza dei dati. I controlli vanno eseguiti regolarmente.

Monitoraggio e controllo degli account: Gestione e monitoraggio degli accessi ai dati personali. Eliminazione degli account sospesi di persone che erano autorizzate al trattamento. La politica di sicurezza dovrebbe designare specifici membri del team per monitorare e controllare attentamente gli account utente, il che impedirebbe il verificarsi di attività illegale.

Segmentazione dei dati e della rete.

COPYRIGHT

Gli utenti non devono copiare software o altri materiali originali provenienti da altre fonti e sono responsabili di tutte le conseguenze che potrebbero derivare dalla legge sulla proprietà intellettuale.

8 ISTRUZIONI OPERATIVE VIDEOSORVEGLIANZA

Codice:	PR08
Revisione:	00
Data della revisione:	18/05/2019

INDICE

PREMESSA

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica; si applicano, pertanto, le disposizioni generali in tema di protezione dei dati personali, volte a garantire l'incolumità pubblica e la sicurezza urbana.

Il Comune di Matera ha adottato una procedura interna per il trattamento dei dati personali acquisiti mediante l'uso di sistemi di videosorveglianza, che rispetta i principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679 e dalla normativa nazionale in vigore.

PRINCIPI GENERALI

La videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

1) protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;
2) protezione della proprietà;
3) rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;
4) acquisizione di prove.

La necessità di garantire, in particolare, un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, purché ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati. Naturalmente l'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, sul controllo a distanza dei lavoratori, in materia di sicurezza presso stadi e impianti sportivi, o con riferimento a musei, biblioteche statali e archivi di Stato, in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano.

L'attività di videosorveglianza dev'essere effettuata nel rispetto del principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite.

DIRITTI DEGLI INTERESSATI

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al regolamento, in particolare il diritto di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento.

Dev'essere assicurato il "diritto all'oblio", ovvero il diritto di ogni singolo individuo a richiedere la cancellazione dei propri dati personali. Vi è, infatti, l'obbligo di cancellazione da parte del titolare del trattamento se sussiste uno dei motivi seguenti: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti

o altrimenti trattati; l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento; l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; i dati personali sono stati trattati illecitamente; i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori" (articolo 17 Regolamento 2016/679 e normativa nazionale in vigore).

ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI

Secondo quanto afferma il Garante per la Privacy, un sistema di videosorveglianza è a norma quando rispetta i principi di liceità, necessità, proporzionalità e finalità. Attraverso il sistema di videosorveglianza è consentita:

- la registrazione delle immagini se necessarie ad obblighi di legge o per tutelare un interesse legittimo (liceità);
- le riprese devono limitarsi solamente a ciò che è necessario per raggiungere gli scopi prefissati (necessità);
- l'impianto va impiegato solo in luoghi dove è realmente necessario, limitando le riprese alle sole aree interessate ed escludendo la visuale su quelle circostanti (proporzionalità);
- lo scopo della videosorveglianza deve essere esplicito e legittimo nonché limitato alle finalità di pertinenza dei titolari dei dati (finalità).

Il principio generale in materia stabilisce che chiunque installi un sistema di videosorveglianza **deve provvedere a segnalarne la presenza**, facendo in modo che qualunque soggetto si avvicini all'area interessata dalle riprese sia avvisato della presenza di telecamere già prima di entrare nel loro raggio di azione.

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata.

Il supporto con l'informativa:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata, poi rinvii a un testo completo contenente tutti gli elementi, accessibile anche con strumenti informatici e telematici.

I**l Titolare del trattamento ha l'obbligo di effettuare la valutazione dell'impatto sulla protezione dei dati personali (DPIA),** nel caso in cui la sorveglianza è sistematica su larga scala di una zona accessibile al pubblico (articolo 35 Regolamento 2016/679 e normativa nazionale in vigore).

VERIFICA PRELIMINARE

Le riprese effettuate per fini di sicurezza e tutela dell'ordine pubblico, con particolare riferimento alla prevenzione di reati o atti di vandalismo e alla sicurezza sul lavoro, costituiscono un'eccezione, e non necessitano dell'obbligo di segnalazione.

Normalmente, per installare un sistema di videosorveglianza, non è necessario l'assenso da parte del Garante della privacy; fanno però eccezione tutti i casi in cui sussiste il rischio di ledere i diritti e le libertà fondamentali o la dignità degli individui ripresi.

Ad esempio, devono essere sottoposti alla verifica preliminare del garante privacy i sistemi di videosorveglianza dotati di *software* **che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate** (es. morfologia del volto) con altri specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima.

Un analogo obbligo sussiste con riferimento a sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso.

La conservazione delle immagini deve avere una durata prestabilita e non eccedente le 24 ore; in situazioni particolari, nelle quali sussiste un elevato fattore di rischio, la durata massima si estende ad una settimana. Nel caso si necessita di una conservazione dei dati più lunga sarà invece necessaria la verifica preliminare del Garante.

Comunque, anche fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati non sono integralmente applicabili, in relazione alla natura dei

dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare.

Esclusione della verifica preliminare

Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza non deve richiedere una verifica preliminare purché siano rispettate tutte le seguenti condizioni:

- il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;
- la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;
- si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti.

Resta altresì inteso che nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza (spesso generici e non valutabili a distanza) cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio-assenso.

È regola generale che non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente.

Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosorveglianza, deve essere preventivamente notificato.

MISURE DI SICUREZZA

Il titolare del trattamento dei dati ha l'obbligo di prendere le misure di sicurezza idonee onde evitare la distruzione, la perdita, l'accesso abusivo alle immagini, nonché il loro utilizzo per scopi incoerenti con le finalità previste.

In particolare, i dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.

Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).

È inevitabile che, in considerazione dell'ampio spettro di utilizzazione di sistemi di videosorveglianza, anche in relazione ai soggetti e alle finalità perseguite nonché della varietà dei sistemi tecnologici utilizzati, le misure minime di sicurezza possano variare anche significativamente.

È tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:

a) **in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini**. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati autorizzati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
c) per quanto riguarda il **periodo di conservazione delle immagini**, devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
d) **nel caso di interventi derivanti da esigenze di manutenzione**, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
e) **qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche**, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;
f) la **trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza**; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi, wi-max, Gprs*).

RESPONSABILI E AUTORIZZATI

Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini. Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori

operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento.

DURATA DELLA CONSERVAZIONE DATI

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario.

Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità, anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario a raggiungere la finalità perseguita.

Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento deve stabilire un termine per la cancellazione o per la verifica periodica.

Generalmente la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che si ritiene non debba comunque superare la settimana.

In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del GARANTE, e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su

tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

SOGGETTI PUBBLICI

I soggetti pubblici sono tenuti a rispettare, al pari di ogni titolare di trattamento effettuato tramite sistemi di videosorveglianza, i principi enunciati.

Anche per i soggetti pubblici sussiste l'obbligo di fornire previamente l'informativa agli interessati. Pertanto, coloro che accedono o transitano in luoghi dove sono attivi sistemi di videosorveglianza devono essere previamente informati in ordine al trattamento dei dati personali. A tal fine, anche i soggetti pubblici possono utilizzare il modello semplificato di informativa che:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Recenti disposizioni legislative in materia di sicurezza hanno attribuito ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidati ad essi dalla legge in materia di sicurezza e di polizia giudiziaria. Al fine di prevenire e contrastare determinati pericoli che minacciano l'incolumità pubblica e la sicurezza urbana, il sindaco può altresì adottare provvedimenti, anche contingibili e urgenti, nel rispetto dei principi generali dell'ordinamento. Infine, il sindaco, quale ufficiale del Governo, concorre ad assicurare la cooperazione della polizia locale con le forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministero dell'interno.

Da tale quadro emerge che sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana.

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze

pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.

Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti.

Avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e da enti territoriali

Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.

L'Autorità ha già individuato un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate, in particolare con riferimento all'attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale.

In particolare:

a) l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente;
b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.

Il titolare del trattamento è tenuto a richiedere una verifica preliminare all'Autorità fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già la richiede (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli).

9. ISTRUZIONE OPERATIVA DATA BREACH

Codice:	PR09
Revisione:	00
Data della revisione:	18/05/2019

L'art. 33 del **Regolamento Europeo 679/2016 (GDPR) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (data breach) entro 72 ore dal momento in cui ne viene a conoscenza.**

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR e della normativa nazionale in vigore.

Per "Violazione di dati" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

È importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

- **violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;**
- **violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;**
- **violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.**

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente: la notifica al Garante non è obbligatoria.**
- **Rischio presente: è necessaria la notifica al Garante.**

- **Rischio elevato: In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.**

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- **coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;**
- **riguardare categorie particolari di dati personali;**
- **comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);**
- **comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);**
- **impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. minori, soggetti indagati).**

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

1. Scopo e Campo di Applicazione

Questa Procedura fornisce i principi generali e un modello di risposta in caso di violazione dei dati personali e sanitari anche al fine di mitigarne gli effetti, in una o in entrambe le seguenti situazioni:

- Il dato personale e particolare o giudiziario identifica gli interessati che risiedono negli Stati Membri dell'Unione Europea (UE) e nelle nazioni all'interno dello Spazio Economico Europeo (SEE), indipendentemente da dove tali dati siano soggetti al trattamento a livello globale;
- I dati personali e sulla salute sono soggetti a trattamento all'interno dell'UE e / o del SEE, indipendentemente dal paese di residenza dell'interessato.

La Procedura definisce i principi e le azioni necessari per gestire con successo la risposta ad una violazione di dati e adempiere agli obblighi relativi alla notifica all'Autorità di controllo e ai singoli interessati, come richiesto dal GDPR dell'UE.

La Procedura deve essere portata a conoscenza, mediante specifica formazione, di tutti i dipendenti - anche temporanei - il personale, i collaboratori e i terzi che lavorano e/o agiscono per conto del Comune di Matera (di seguito "l'Amministrazione") i quali sono tenuti a seguirla in caso di violazione dei dati personali.

2. Documenti di Riferimento

- GDPR dell'UE 2016/679 (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE); Politica sulla Protezione dei Dati Personali;
- Linee guida pubblicate dal Gruppo di lavoro 29 (di seguito WP29);
- FAQ pubblicate dal Garante per la Protezione dei Dati Personali (Garante Privacy).
- D.Lgs. 193/2003 come modificato del D.Lgs. 101/2018

3. Definizioni

Le seguenti definizioni sono tratte dall'articolo 4 del Regolamento Generale sulla Protezione dei Dati dell'Unione europea (o GDPR):

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

"**Dato relativo alla Salute**" o "**dato sanitario**": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rilevano informazioni relative al suo stato di salute passato, presente e futuro;

"**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.

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

"**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.

"**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.

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

4. Gruppo di Risposta alle Violazioni dei Dati

Il Gruppo di Risposta alle Violazioni dei Dati personali (di seguito "Gruppo") è costituito da più **persone esperte e c**ompetenti IT, Risk Managment, Sicurezza Informatica, Diritto e Affari Legali.

Con atto separato e specifico vengono nominati il Responsabile e i membri del Gruppo di Risposta alle Violazioni dei Dati. Il Gruppo, in linea con il principio di *Privacy by design,* è nominato a prescindere dal fatto che una violazione sia o meno a*vv*enuta.

Gruppo fornisce una risposta immediata, efficace ed esperta a qualsiasi sospetta, presunta o effettiva violazione dei dati personali e/o sanitari che riguardi l'Amministrazione.

A tal fine, i componenti del Gruppo sono individuati tra i soggetti che garantiscono la preparazione necessaria per adempiere all'incarico conferito. Al Gruppo sono assegnate risorse adeguate allo svolgimento del proprio incarico.

Il Gruppo può trattare più di una violazione dei dati personali e/o particolari sospetta, presunta o effettiva alla volta.

Il Responsabile del Gruppo può scegliere di inserire personale aggiuntivo o coinvolgere parti esterne (ad es.: un fornitore di sicurezza informatica per svolgere attività d'informatica forense, oppure, un'agenzia di comunicazione esterna per assistere l'Amministrazione in necessità di comunicazione di crisi) allo scopo di gestire una specifica violazione dei dati personali.

Il Gruppo è incaricato di rispondere ad ogni violazione dei dati personali e/o particolari, sospetta, presunta o effettiva, 24 ore su 24, 7 giorni su 7, per tutto l'anno. A tal fine, le informazioni di contatto di ciascun membro del Gruppo, inclusi i dati personali, saranno

archiviate in un sito centrale interno ed utilizzati per riunire il Gruppo ad ogni notizia di sospetta, presunta o effettiva violazione dei dati personali e/o particolari.

5. I compiti del Gruppo di Risposta alle Violazioni dei Dati

Il Gruppo si riunisce, anche virtualmente, a seguito di segnalazioni di violazione dei dati personali e/o particolari, sospetta, presunta o effettiva; è coordinato dal Responsabile del Gruppo e, ove il rischio per i diritti e le libertà delle persone risulta elevato, è guidato dal Data Protection Officer.

Il Gruppo:

Valuta il livello di rischio derivante dalla violazione dei dati personali; Identifica i requisiti per la risoluzione delle violazioni e ne monitora la concreta applicazione.

Il Responsabile del Gruppo, o chi ne fa le veci, nello svolgimento della sua funzione di coordinamento:

- Assicura che sia avviata, condotta, documentata e conclusa un'indagine corretta e imparziale (compresa l'informatica forense, se necessario);
- Riferisce i risultati all'alta Direzione;
- Provvede al coordinamento con le Autorità competenti se necessario;
- Coordina le comunicazioni interne ed esterne;
- Garantisce che gli interessati siano adeguatamente informati, se necessario.

6. Il Processo di Risposta alle Violazione dei Dati

La Procedura di Risposta alle Violazione dei Dati è avviata nel momento in cui un qualsiasi membro del Gruppo sia notiziato di una sospetta, presunta o effettiva violazione dei dati personali e/o particolari da parte di un qualsiasi dipendente, collaboratore o terzo, che lavora o agisce per conto dell'Amministrazione, oltre che dal soggetto interessato e, comunque, a prescindere dalla fonte.

Qualsiasi dipendente, collaboratore o terzo che lavora o agisce per conto dell'Amministrazione è tenuto a comunicare al componente del Gruppo di prima e pronta reperibilità la notizia di una sospetta, presunta o effettiva violazione dei dati personali e/o particolari.

Il Gruppo è responsabile della determinazione del grado di complessità e del rischio relativo alla violazione, pertanto, laddove il caso risulti complesso, chiede un parere al DPO.

Il Responsabile del Gruppo è incaricato della corretta tenuta della documentazione di tutte le decisioni del Gruppo, poiché, tale documentazione potrebbe essere oggetto di esame da parte dall'Autorità di Controllo. Pertanto, i documenti devono essere redatti in modo preciso, accurato e dettagliato al fine di garantire la tracciabilità del lavoro svolto e la responsabilizzazione di chi vi ha operato (accountability).

7. Notifica di una violazione dei dati personali e/o sanitari da parte dell'Amministrazione, nella qualità di Responsabile del trattamento, al Titolare del trattamento

Se la violazione dei dati personali e/o particolari, presunta o sospetta, riguarda i dati elaborati/trattati dall'Amministrazione per conto di terzi, il Gruppo lo comunica senza ritardo al DPO, il quale tempestivamente lo notifica al Titolare del trattamento, includendo:

- Una descrizione della natura della violazione;
- Le categorie dei dati personali in questione;
- Il numero approssimativo degli interessati;
- Il nome e le informazioni di contatto del Responsabile del Gruppo di Risposta alle Violazioni;
- Le conseguenze della violazione dei dati personali e/particolari;
- Le misure adottate per gestire la violazione dei dati personali e/o particolari;
- Qualsiasi informazione relativa alla violazione dei dati.

La violazione dei dati è annotata nel Registro delle Violazioni dei dati dal Responsabile del Gruppo o da altro membro funzionalmente e formalmente incaricato dall'Amministrazione.

8. Notifica di una violazione dei dati da parte dell'Amministrazione, nella qualità di Titolare del trattamento, all'Autorità di controllo

Quando la violazione dei dati personali e/o particolari, presunta, sospetta o effettiva riguarda i dati trattati dall'Amministrazione, come Titolare del trattamento, si procede nel seguente modo:

1) Il Gruppo stabilisce se la violazione dei dati personali e/o particolari è in grado di mettere in pericolo i diritti e le libertà degli interessati e, di conseguenza, se deve o meno essere segnalata all'Autorità di controllo. Al fine di determinare il rischio per i diritti e le

libertà dell'interessato in questione, il Gruppo coadiuvato dal DPO esegue la Valutazione d'Impatto sulla Protezione dei Dati relativa all'attività di trattamento interessata dalla violazione stessa.

2) Se la violazione dei dati personali e/o particolari non comporta un rischio per i diritti e le libertà degli interessati, non si procede ad alcuna notifica.

Cionondimeno, la violazione dei dati è registrata, documentata e conservata per un tempo ragionevole; Quando la violazione dei dati personali e/o particolari pone a rischio i diritti e le libertà degli interessati, l'Autorità di Controllo deve essere informata senza indebito ritardo e, comunque, non oltre le 72 ore. Qualora la notifica non avvenga entro i suddetti termini deve darsi atto delle ragioni che abbiano comportato il giustificato ritardo.

La notifica all'Autorità di Controllo, inviata dal Responsabile del Gruppo o da chi ne fa le veci, deve includere:

- Una descrizione della natura della violazione;
- Le categorie dei dati personali e/o particolari in questione;
- Il numero approssimativo degli interessati;
- Il nome e le informazioni di contatto del Responsabile del Gruppo e del DPO;
- Le conseguenze della violazione dei dati personali e/o particolari;
- Le misure adottate per gestire la violazione dei dati personali e/o particolari;
- Qualsiasi ulteriore informazione relativa alla violazione dei dati.

9. Comunicazione di una violazione dei dati personali da parte dell'Amministrazione, nella qualità di Titolare del trattamento, all'interessato

Il Gruppo valuta se la violazione dei dati personali e/o particolari comporta un rischio elevato per i diritti e le libertà dell'interessato. In caso affermativo, il DPO informa il titolare del Trattamento che a sua volta informa gli interessati senza indebito ritardo.

La comunicazione agli interessati deve essere scritta con modalità di linguaggio chiaro e semplice e deve contenere le stesse informazioni elencate nella Sezione precedente e, in aggiunta, l'indicazione delle misure consigliate che possono essere messe in atto dal medesimo interessato al fine di limitare gli effetti negativi.

Se a causa del numero degli interessati risulta sproporzionatamente complesso informare tutti i soggetti in questione, il Responsabile del Gruppo deve adottare le misure necessarie per garantire che le persone interessate siano informate utilizzando anche canali appropriati e pubblicamente disponibili.

10. Responsabilizzazione

Qualsiasi dipendente, collaboratore o terzo che agisca per conto dell'Amministrazione e violi la presente Procedura è soggetto a misure disciplinari interne; inoltre, qualora le sue azioni violino la legge, potrebbe incorrere in responsabilità civile o penale.

11. FLUSSO OPERATIVO

Sono di seguito riepilogati i passaggi operativi ed i comportamenti da adottare per una corretta gestione di una violazione dei dati personali riscontrata:

Qualora un Soggetto Autorizzato e/o un Amministratore di Sistema ritenga che sia in corso o vi sia il concreto rischio che si verifichi (o si sia già verificata) una violazione dei dati personali, deve tempestivamente e senza ritardo coinvolgere il DPO e il Gruppo di Lavoro.

a) La segnalazione deve avvenire con una mail all'indirizzo mail del DPO o di uno dei Referenti infividuati dall'Amministrazione (meglio se lo scambio avvenisse tra due caselle pec). In ogni caso deve essere certa l'immediata ricezione dell'informazione da parte del destinatario.
b) Il DPO o il Referente privacy interno convocano in tempi utili e in un tempo ragionevole e non più di 12 h il gruppo di lavoro.
c) Il Gruppo di lavoro compie una prima valutazione circa la natura della segnalazione.
d) Qualora si tratti di una violazione di dati personali o sia stata riscontrata la concreta minaccia che la stessa si verifichi, il Referente Interno informa senza indugio il Titolare del trattamento.
e) Il Titolare, coadiuvato dal Gruppo di Lavoro e dal DPO compie una valutazione maggiormente approfondita dell'incidente secondo i seguenti criteri:
    - Natura della violazione dei dati personali
    - (Ove possibile) il numero – anche approssimativo – di interessati coinvolti
    - (Ove possibile) le categorie ed il numero -anche approssimativo- di dati personali coinvolti
    - Probabili conseguenze della violazione
f) A seguito di tale valutazione il Titolare e i soggetti coinvolti individuano e -se del caso- adottano le misure adeguate per porre rimedio alla violazione o per attenuarne i possibili effetti negativi.
g) Il DPO aggiorna il Registro delle violazioni.

h) Il Titolare notifica al Garante secondo le procedure all'uopo disposte dall'Autorità e -se del caso- procede alla Notificazione agli interessati secondo i modelli predisposti dal Garante e/o approvati dall'ente.

12. Validità e gestione del documento

Questo documento è valido ed efficace a partire dall'adozione della relativa deliberazione.

Il Referente interno riguardo questo documento è individuato nel _____, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.

13. Riesame

Periodicamente e almeno ogni sei mesi tutte le attività relative alle violazioni, saranno soggette a riesame al fine di migliorare il sistema di gestione dei dati personali. I report forniranno la base per indirizzare i futuri investimenti in materia di sicurezza delle informazioni e indicazioni per modifiche e adeguamenti tecnici e costituiranno un input del processo di analisi dei rischi. In particolare, i gravi incidenti sulla violazione dei dati personali, quelli con impatti alti, impongono un immediato aggiornamento e ricalcolo del rischio.

STEP	ATTIVITA'	CHI	A CHI	QUANDO	COME
1	Rilevazione e segnalazione di data breach	Tutto il personale, collaboratori, fornitori, responsabili	Ad una figura interna del Gruppo di Risposta o al DPO. n mancanza di uno qualsiasi di questi soggetti una figura incaricata all'uopo dal Titolare del Trattamento	Appena se ne viene a conoscenza	Utilizzando le vie più brevi (telefono, di persona, e-mail meglio pec). Comunque bisognerà essere certi della ricezione del messaggio.
2	Raccolta informazioni sulla violazione	Il Gruppo di Risposta insieme al DPO. In mancanza di uno qualsiasi di questi soggetti una		Immediatamente	Utilizzando il modello fornito e raccogliendo informazioni dai soggetti coinvolti nella segnalazione e nel trattamento

		figura incaricata all'uopo dal Titolare del Trattamento			**dei dati violati. Utilizzando uno dei metodi ufficialmente disponibili e utilizzando** *una specifica tecnica, adottata da un organismo di normazione riconosciuto, tipo Metodo ENISA*
3	**Comunicazione del data breach**	**Il gruppo di Risposata e/o il data breach o In mancanza di uno qualsiasi di questi soggetti una figura incaricata all'uopo dal Titolare del Trattamento**	**Al titolare del trattamento**	**Appena ottenute informazioni di base sulla violazione**	**Utilizzando le vie più brevi (telefono, di persona, e-mail meglio pec). Comunque bisognerà essere certi della ricezione del messaggio.**
	Valutazione d'impatto	**Titolare, RPD, esperti ICT, soggetti coinvolti**		**Appena ricevuta la comunicazione**	**Utilizzando la metodologia indicata nel piano della protezione dei dati personali e gestione dei rischi o uno dei metodi ufficialmente disponibili e utilizzando** *una specifica tecnica, adottata da un organismo di normazione riconosciuto, tipo Metodo ENISA*
	Individuazione delle azioni correttive	**DPO – Gruppo di Risposta**		**Appena terminata la valutazione d'impatto**	**Analizzando i risultati della valutazione d'impatto**
	Comunicazione delle valutazioni effettuate e delle azioni da intraprendere	**DPO – Gruppo di Risposta**	**Al Titolare**		**Tramite una breve relazione anche orale**
	Notifica della violazione (se è necessaria)	**Titolare**	**Al Garante**	**Entro 72 ore dalla rilevazione**	**Mediante la modulistica predisposta dal Garante**
	Comunicazione agli interessati coinvolti (se è necessaria)	**Titolare**	**Alle persone fisiche i cui dati sono stati**	**Nei termini indicati nella valutazione**	**Comunicazione diretta alle singole persone o mediante**

			violati	**d'impatto**	**pubblicazione in sito a loro accessibile delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate**
	Disposizioni per l'attuazione delle misure correttive (se individuate)	**Gruppo di Risposta, Responsabili delle strutture coinvolte**	**Ai soggetti incaricati di svolgere le attività**	**Nei termini indicati nella valutazione d'impatto**	**Devono essere indicate in dettaglio le operazioni da svolgere, chi è l'incaricato, i tempi di attuazione; prevedere eventuali operazioni di verifica dell'efficacia delle misure correttive**
	Recepimento della risposta del Garante alla notifica (se effettuata)	**Titolare, DPO, responsabili delle strutture coinvolte, esperti ICT**			**Disposizioni per l'attuazione delle eventuali misure correttive indicate dal Garante; effettuazione di ulteriori indagini per approfondire le informazioni raccolte**

Attività relative alla registrazione dell'incidente

STEP	ATTIVITA'	CHI	QUANDO	COME
1	Registrazione della violazione/aggiornamenti	Referente del Registro delle violazioni	Appena ricevuta la comunicazione	Compilando l'apposito registro con la descrizione della violazione, delle azioni intraprese e annotando i successivi aggiornamenti.
2	Registrazione della risposta del Garante	Referente del Registro delle violazioni	Al momento della ricezione	Annotando sul registro gli estremi della risposta del Garante e le eventuali prescrizioni in essa contenute
3	Registrazione della prosecuzione/chiusura	Referente del Registro delle	In seguito alle indicazioni del	Registra la chiusura dell'incidente se

	dell'incidente	violazioni	DPO	non necessita di ulteriori indagini o riporta le istruzioni per le ulteriori indagini

Attività inerenti la prosecuzione delle indagini

STEP ATTIVITA'		CHI	A CHI	QUANDO	COME
1	Prosecuzione delle indagini	DPO, responsabile della struttura o sostituto o incaricato privacy, soggetti coinvolti nella violazione e nei trattamenti di dati violati, esperti ICT		A seguito di indicazione da parte del Garante o del titolare; se previsto nella prima valutazione d'impatto; nel caso che le informazioni raccolte risultino incomplete o mancanti	Raccogliendo le informazioni mancanti, o approfondendo quelle note per rilevare eventuali impatti non riscontrati nella prima indagine
2	Esecuzione di una nuova valutazione d'impatto	Titolare, DPO, esperti ICT, soggetti coinvolti, Gruppo di Risposta		Al momento che si ritiene di aver raccolto tutte le informazioni possibili sulla violazione	
3	Comunicazione dei risultati del proseguimento delle indagini	DPO, responsabile della struttura o sostituto o incaricato privacy	Al Titolare	appena terminato il lavoro	Tramite relazione sintetica sui risultati della valutazione d'impatto e sulle azioni necessarie, allegando il materiale informativo raccolto
4	Aggiornamento della notifica al Garante (se necessario)	Titolare sentito il DPO	Al Garante	Appena sono disponibili i nuovi dati o secondo i termini stabiliti dal Garante	Mediante la modulistica predisposta o come indicato dal Garante
5	Comunicazioni agli interessati (se necessario)	Titolare sentito il DPO e il Gruppo di Risposta		Nei tempi stabiliti nella valutazione d'impatto	Contattando direttamente gli interessati oppure rendendo nota la violazione e le possibili conseguenze mediante pubblicazione accessibile alle

					categorie di interessati

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

NON OSSERVANZA DELLA NORMATIVA

Il mancato rispetto o la violazione delle regole contenute nel presente manuale è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente manuale.

Il presente manuale è soggetto a revisione con frequenza annuale.

10. POLITICA DELLA SCRIVANIA PULITA E DELLO SCHERMO PULITO

Codice:	PR10
Revisione:	00
Data della revisione:	18/05/2019

SCOPO, CAMPO DI APPLICAZIONE E UTENTI

Lo scopo di questo documento è quello di definire le regole per impedire l'accesso non autorizzato alle informazioni nei luoghi di lavoro, nonché alle strutture e alle attrezzature condivise.

Questo documento si applica a tutti i luoghi di lavoro, le strutture e le attrezzature situate all'interno delle sedi del Comune di Matera

Destinatari di questo documento sono tutti dipendenti del Comune di Matera.

Protezione della scrivania (Clear desk policy)

Se la persona autorizzata non è alla sua postazione di lavoro, tutti i documenti cartacei e i supporti di memorizzazione dei dati contrassegnati come particolari, devono essere rimossi dalla scrivania o da altri luoghi (stampanti, fax, fotocopiatrici, ecc.) per impedire la visualizzazione e l'accesso a personale non autorizzato.

Tali documenti e supporti devono essere immagazzinati in modo sicuro secondo la Politica sulla classificazione dei dati.

Clear screen policy

Se la persona autorizzata non è alla sua postazione di lavoro, tutte le informazioni sensibili devono essere rimosse dallo schermo e l'accesso deve essere negato a tutti i sistemi per i quali la persona ha l'autorizzazione.

In caso di breve assenza (fino a 10 minuti), la politica dello schermo pulito viene implementata disconnettendo tutti i sistemi o bloccando lo schermo con una password. Se la persona è assente per un periodo di tempo più lungo (oltre 15 minuti), la politica dello schermo pulito viene implementata disconnettendo tutti i sistemi attraverso il reboot della workstation.

Protezione delle strutture e delle attrezzature condivise

I documenti contenenti informazioni sensibili devono essere immediatamente rimossi dalle stampanti, dalle macchine per il fax e dalla copia.

Fotocopiatrici multifunzione, nonché le strutture per la spedizione e la ricezione della posta, devono essere protette quando la persona autorizzata è assente, ad esempio chiudendo la porta di accesso ai locali a chiave.

L'uso non autorizzato di stampanti, fotocopiatrici, scanner e altre apparecchiature condivise per la copia deve essere impedito attraverso l'utilizzo di numeri PIN.

11. POLITICA PER I DISPOSITIVI MOBILE E IL TELELAVORO

Codice:	PR11
Revisione:	00
Data della revisione:	18/05/2019

SCOPO, CAMPO DI APPLICAZIONE E UTENTI

Lo scopo di questo documento è quello di definire come il Comune di Matera conserverà il controllo sulle sue informazioni nelle ipotesi in cui tali informazioni siano accessibili tramite dispositivi mobili di proprietà dell'organizzazione e dispositivi di proprietà personale.

Questo documento è applicato a tutti i dispositivi di proprietà del Comune di Matera che hanno la capacità di memorizzare, trasferire o elaborare informazioni che contengono dati personali. Detti dispositivi includono computer portatili, smartphone, tablet, memory stick USB, fotocamere digitali, ecc.

Destinatari di questo documento sono tutti dipendenti del Comune di Matera e tutti i possibili fornitori o altra ditta che venga ad avere rapporti con il Comune di Matera.

NORME DI SICUREZZA PER L'UTILIZZO DEI DISPOSITVI E TELELAVORO

Le norme di questa Politica si applicano a tutti i dispositivi mobili di proprietà del Comune di Matera assegnati al dipendente e a tutti i dispositivi mobili personali autorizzati, indipendentemente dal fatto che siano usati per lavoro o per uso privato o siano utilizzati all'interno o all'esterno dei locali dell'organizzazione, solo dopo aver ottenuto apposita autorizzazione scritta da parte del *Responsabile dei sistemi informatici*.

POLITICA INTERNA

L'organizzazione autorizza l'uso anche in aree al di fuori degli uffici di dispositivi mobili di proprietà dell'organizzazione per l'esecuzione della propria attività lavorativa.

L'organizzazione autorizza l'uso di dispositivi mobili per uso professionale, ovvero l'utilizzo di tali dispositivi per l'esecuzione di lavori anche in aree al di fuori degli uffici.

I dati memorizzati, trasferiti o elaborati tramite l'utilizzo di dispositivi mobili, rimangono sotto la proprietà dell'organizzazione e la stessa conserva il diritto di controllare tali dati anche se non è proprietario del dispositivo.

USO ACCETTABILE

La fornitura di accesso dovrà avvenire in **modalità desktop virtuale** che prevenga l'elaborazione e la memorizzazione di informazioni su dispositivi privati;

L'Autorizzato dovrà attuare tutte le misure idonee a prevenire le minacce di accesso non autorizzato alle informazioni o alle risorse da parte di altri soggetti che frequentano il luogo, per esempio i famigliari e gli amici;

Conformarsi alle politiche e alle procedure per prevenire discussioni riguardo i diritti per la proprietà intellettuale sviluppatisi su dispositivi privati;

Accordare l'accesso a dispositivi privati (per verificare la sicurezza del sistema o durante un'indagine);

Adottare tutte le cautele affinché il sistema sia protetto da malware non disattivando l'antivirus fornito dall'organizzazione e mantenendolo costantemente aggiornato.

Adottare le seguenti cautele:

- Quando si utilizza il dispositivo mobile al di fuori della sede, non deve essere lasciato incustodito e, se possibile, deve essere bloccato fisicamente;
- quando si utilizza il dispositivo mobile in luoghi pubblici, il proprietario o l'assegnatario deve prestare la massima attenzione affinché' i dati non vengano letti da persone non autorizzate;
- le patch e gli aggiornamenti devono essere installati regolarmente;
- la persona che utilizza apparecchiature informatiche mobili sede sarà collegato con VPN e desktop remoto e pertanto lavorerà direttamente sui Server con un profilo dedicato.
- le informazioni sui computer portatili devono essere cifrate per l'intero disco rigido.
- comunicare immediatamente tramite e-mail al DPO e all'Amministratore di Sistema l'eventuale furto, smarrimento, distruzione del dispositivo mobile aziendale e/o del dispositivo mobile personale.

Non è permesso:

- installare applicazioni non rilasciate dal Servizio IT;
- conservare materiali illegali sul dispositivo;
- installare software non autorizzato o privo di licenza;
- connettersi a reti Wi-Fi sconosciute;
- memorizzare in locale le password;
- trasferire dati dell'organizzazione su altri dispositivi che non sono consentiti.

DIRITTI SPECIALI

Comune di Matera ha il diritto di visualizzare, modificare ed eliminare tutti i dati memorizzati, trasferiti o elaborati su dispositivi mobili e revocare l'utilizzo.

L’Amministratore di Sistema è autorizzato a configurare qualsiasi dispositivo mobile in base a questa politica e monitorarne l'uso.

12. POLITICA PER IL CONTROLLO DEGLI ACCESSI

Codice:	PR12
Revisione:	00
Data della revisione:	18/05/2019

SCOPO, CAMPO DI APPLICAZIONE E UTENTI

Lo scopo di questo documento è quello di definire le regole per l'accesso a vari sistemi, attrezzature, strutture e informazioni, basati su requisiti di sicurezza per l'accesso, anche archivi fisici.

CONTROLLO DEGLI ACCESSI

Il principio fondamentale è che l'accesso a tutti i sistemi, le reti, i servizi e le informazioni è vietato, salvo che non sia espressamente consentito a singoli utenti o gruppi di utenti. Viene predisposta una procedura di registrazione degli utenti per ogni sistema e servizio.

È consentito l'accesso a tutte le aree fisiche dell'organizzazione, ad eccezione delle aree per le quali il privilegio deve essere concesso dalla persona autorizzata (voce "Gestione privilegi").

Questa politica specifica le regole per l'accesso a sistemi, servizi e strutture, mentre la Politica per la classificazione dei dati definisce le regole per l'accesso a singoli documenti.

Profilo utente A

Il profilo utente A ha i seguenti diritti di accesso:

Nome del sistema / rete / servizio /Archivio	***Diritti degli utenti [lettura, scrittura, cancellazione, modifica e/o svolgimento di funzioni specifiche, Presa in carico]***

Profilo utente B

Il profilo utente B ha i seguenti diritti di accesso:

Nome del sistema / rete / servizio	***Diritti degli utenti [lettura, scrittura, cancellazione, modifica e/o svolgimento di funzioni specifiche, Presa in carico]***

Gestione dei privilegi

I privilegi relativi ai suddetti profili utente (concessione o rimozione dei diritti di accesso) vengono assegnati nel modo seguente:

Nome del sistema / rete / servizio / area fisica	***Chi è autorizzato a concedere o rimuovere i diritti di accesso***	***Forma del processo di autorizzazione***

Revisione periodica dei diritti di accesso

I proprietari di ciascun sistema e delle strutture per i quali sono richiesti diritti speciali di accesso devono, nei seguenti intervalli, verificare se i diritti di accesso concessi siano in linea con i requisiti dell'organizzazione e di sicurezza:

Nome del sistema / rete / servizio / area fisica	*Intervalli della revisione periodica [la frequenza deve essere definita tenendo in considerazione il livello di rischio associato al sistema basato sui risultati della valutazione del rischio]*

Ogni revisione deve essere registrata.

Cambiamento di stato o risoluzione del contratto

In caso di cambiamento del rapporto di lavoro o di cessazione del rapporto di lavoro, il Titolare del Trattamento deve immediatamente informare le persone responsabili che hanno approvato i privilegi per il dipendente in questione.

In caso di cambiamento dei rapporti contrattuali con soggetti esterni che hanno accesso a sistemi, servizi e strutture o alla scadenza del contratto, il proprietario del contratto deve immediatamente informare le persone responsabili che hanno approvato i privilegi per i soggetti esterni in questione.

I diritti di accesso per tutte le persone che hanno modificato il loro status di lavoro o la loro relazione contrattuale devono essere immediatamente rimosse o modificate dalle persone responsabili come definito nella sezione successiva.

Realizzazione tecnica

L'esecuzione tecnica dell'assegnazione o della rimozione dei diritti di accesso è effettuata dalle seguenti persone:

Nome del sistema / rete / servizio / area fisica	*Persona responsabile dell'implementazione*

Le persone elencate in questa tabella non possono concedere o cancellare liberamente i diritti di accesso, ma solo in base ai profili utente definiti nella presente Policy e alle richieste di persone autorizzate per l'assegnazione dei privilegi.