LIBERO CONSORZIO COMUNALE DI RAGUSA

SETTORE 1

DETERMINAZIONE

Registro generale n. **195/2024**	**OGGETTO:** SETTORE 1. INDIVIDUAZIONE E NOMINA DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 29 DEL GDPR.
Registro di settore n. **34/2024**	

Premesso:

- il Regolamento U.E. 679/2016 del Parlamento Europeo e del Consiglio (GDPR - General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- la Deliberazione del Commissario straordinario, con i poteri del Consiglio, ex art 51 della LR 15/2015 avente per oggetto "Adozione del regolamento di attuazione del regolamento UE 2016/679 relativo alla protezione delle persone fisiche on riguardo al trattamento dei dati personali"

Considerata la struttura organizzativa e l'organigramma funzionale degli Uffici e dei servizi;

Considerato che occorre dare corso all'adeguamento gestionale, organizzativo, documentale e procedurale necessario per garantire la sicurezza dei dati conformemente alle disposizioni del GDPR;

Rilevato che, ai fini dell'adeguamento e del rispetto della normativa europea e nazionale in materia di trattamento dei dati, occorre monitorare ed aggiornare gli atti di nomina dei soggetti autorizzati:

UOC 1				
Nr	**Nome**	**Cognome**	**Ruolo ricoperto**	**Area Professionale**
1	RAFFAELE	FALCONIERI	Dirigente	
2	ANTONIO	CARBONARO	ispettore superiore di polizia provinciale	Funzionario ed E.Q.
3	EMANUELE	CASTELLO	ispettore superiore di polizia provinciale	Funzionario ed E.Q.
4	CARMELO	DI ROSA	ispettore superiore di polizia provinciale	Funzionario ed E.Q.
5	ANTONIO	TERRIBILE	ispettore superiore di polizia provinciale	Funzionario ed E.Q.
6	VINCENZO	VINDIGNI	ispettore superiore di polizia provinciale	Funzionario ed E.Q.
7	VINCENZO	BARONE	agente polizia provinciale	Istruttore
8	ROBERTO	BOCCHIERI	agente polizia provinciale	Istruttore
9	GIOVANNI	BRAFA	agente polizia provinciale	Istruttore
10	ANTONIO	CARUSO	agente polizia provinciale	Istruttore
11	CARMELO	PARRINO	agente polizia provinciale	Istruttore
12	LUIGI	SANTORO	agente polizia provinciale	Istruttore
13	SALVATORE	TERRANOVA	agente polizia provinciale	Istruttore

14	MICHELE	CAVARRA	agente polizia provinciale	Istruttore
15	STEFANO	CASTELLO	agente polizia provinciale	Istruttore
16	VIVIANA	GIARDINA	agente polizia provinciale	Istruttore
17	LINDA	OTTONE	agente polizia provinciale	Istruttore
18	GIANNA	CARFI'	istruttore amministrativo	Istruttore
19	SALVATORE	MUCCIO	collaboratore amministrativo	operatore esperto
20	PAOLO	MONCADA	collaboratore tecnico	operatore esperto

UOC 2				
Nr	**Nome**	**Cognome**	**Ruolo Ricoperto**	**Area Professionale**
1	MARIA	MARTORANA	funzionario amministrativo	Funzionario ed E.Q.
2	GIOVANNA	MIGLIORISI	istruttore amministrativo	Istruttore
3	MARIA	MANTICELLO	collaboratore amministrativo	Operatore Esperto
4	GIOVANNA	CAPPUZZELLO	collaboratore amministrativo	Operatore Esperto
5	ANTONIETTA	FIRRINCIELI	collaboratore amministrativo	Operatore Esperto
6	LUCIA	IACONO	collaboratore amministrativo	Operatore Esperto
7	MARIA	NOBILE	collaboratore amministrativo	Operatore Esperto
8	IVANA	MERCORILLO	collaboratore amministrativo	Operatore Esperto
9	GIOVANNI	MINARDO	collaboratore amministrativo	Operatore Esperto

UOC 3				
Nr	**Nome**	**Cognome**	**Ruolo Ricoperto**	**Area professionale**
1	CONCETTA	TORO	funzionario professionale contabile	Funzionario ed E.Q.
2	MARIA	MASSARI	collaboratore amministrativo	Operatore Esperto
3	FRANCESCA	CARBONE	collaboratore amministrativo	Operatore Esperto
4	MARIA GRAZIA	IURA	collaboratore amministrativo	Operatore Esperto
5	VITA	LACOGNATA	collaboratore amministrativo	Operatore Esperto

UOC 4				
Nr	**Nome**	**Cognome**	**Ruolo Ricoperto**	**Area Professionale**
1	CARMELA	CIMINO	funzionario professionale amministrativo	Funzionario ed E.Q.
2	MARIACONCETTA	POMILLO	funzionario contabile	Funzionario ed E.Q.

Rilevato che

- i dipendenti sopra menzionati gestiscono, per l'attività strettamente rientrante nelle proprie funzioni, i processi/procedimenti dell'Ufficio;
- la presente nomina viene effettuata in relazione alle operazioni di elaborazione di dati personali ai quali i soggetti Autorizzati hanno accesso nell'espletamento della funzione che è loro propria. In particolare non è consentito l'accesso a dati la cui conoscenza non è necessaria all'adempimento dei compiti affidati agli Autorizzati.

Considerato che non sussiste in capo al sottoscritto Dirigente alcun conflitto di interesse, anche potenziale, in ordine al presente procedimento.

IL DIRIGENTE

Vista la superiore premessa e narrativa
Considerato che la stessa è conforme alle disposizioni di legge e ai regolamenti attualmente vigenti.
Considerato che non sussiste in capo al sottoscritto Dirigente alcun conflitto di interesse, anche potenziale, in ordine al presente procedimento.
Visto il Regolamento U.E. 679/2016 del Parlamento Europeo e del Consiglio (GDPR - General Data Protection Regulation)

Per le motivazioni di cui sopra, con decorrenza immediata e fino a nuova disposizione:

D E T E R M I N A

1) INDIVIDUARE E NOMINARE "Autorizzati al trattamento" dei dati personali inerenti i servizi ed uffici facenti capo al sottoscritto Dirigente e/o realizzati per conto dell'Ente, il personale interno di seguito indicato:

UOC 1				
Nr	**Nome**	**Cognome**	**Ruolo ricoperto**	**Area Professionale**
1	RAFFAELE	FALCONIERI	Dirigente	
2	ANTONIO	CARBONARO	ispettore superiore di polizia provinciale	Funzionario ed E.Q.
3	EMANUELE	CASTELLO	ispettore superiore di polizia provinciale	Funzionario ed E.Q.
4	CARMELO	DI ROSA	ispettore superiore di polizia provinciale	Funzionario ed E.Q.
5	ANTONIO	TERRIBILE	ispettore superiore di polizia provinciale	Funzionario ed E.Q.
6	VINCENZO	VINDIGNI	ispettore superiore di polizia provinciale	Funzionario ed E.Q.
7	VINCENZO	BARONE	agente polizia provinciale	Istruttore
8	ROBERTO	BOCCHIERI	agente polizia provinciale	Istruttore
9	GIOVANNI	BRAFA	agente polizia provinciale	Istruttore
10	ANTONIO	CARUSO	agente polizia provinciale	Istruttore
11	CARMELO	PARRINO	agente polizia provinciale	Istruttore
12	LUIGI	SANTORO	agente polizia provinciale	Istruttore
13	SALVATORE	TERRANOVA	agente polizia provinciale	Istruttore
14	MICHELE	CAVARRA	agente polizia provinciale	Istruttore
15	STEFANO	CASTELLO	agente polizia provinciale	Istruttore
16	VIVIANA	GIARDINA	agente polizia provinciale	Istruttore
17	LINDA	OTTONE	agente polizia provinciale	Istruttore
18	GIANNA	CARFI'	istruttore amministrativo	Istruttore
19	SALVATORE	MUCCIO	collaboratore amministrativo	operatore esperto
20	PAOLO	MONCADA	collaboratore tecnico	operatore esperto

UOC 2				
Nr	**Nome**	**Cognome**	**Ruolo Ricoperto**	**Area Professionale**
1	MARIA	MARTORANA	funzionario amministrativo	Funzionario ed E.Q.
2	GIOVANNA	MIGLIORISI	istruttore amministrativo	Istruttore
3	MARIA	MANTICELLO	collaboratore amministrativo	Operatore Esperto
4	GIOVANNA	CAPPUZZELLO	collaboratore amministrativo	Operatore Esperto
5	ANTONIETTA	FIRRINCIELI	collaboratore amministrativo	Operatore Esperto
6	LUCIA	IACONO	collaboratore amministrativo	Operatore Esperto
7	MARIA	NOBILE	collaboratore amministrativo	Operatore Esperto
8	IVANA	MERCORILLO	collaboratore amministrativo	Operatore Esperto
9	GIOVANNI	MINARDO	collaboratore amministrativo	Operatore Esperto

UOC 3				
Nr	**Nome**	**Cognome**	**Ruolo Ricoperto**	**Area professionale**
1	CONCETTA	TORO	funzionario professionale contabile	Funzionario ed E.Q.
2	MARIA	MASSARI	collaboratore amministrativo	Operatore Esperto
3	FRANCESCA	CARBONE	collaboratore amministrativo	Operatore Esperto
4	MARIA GRAZIA	IURA	collaboratore amministrativo	Operatore Esperto
5	VITA	LACOGNATA	collaboratore amministrativo	Operatore Esperto

UOC 4				
Nr	**Nome**	**Cognome**	**Ruolo Ricoperto**	**Area Professionale**
1	CARMELA	CIMINO	funzionario professionale amministrativo	Funzionario ed E.Q.
2	MARIACONCETTA	POMILLO	funzionario contabile	Funzionario ed E.Q.

2) DARE ATTO CHE:

- Ciascun soggetto autorizzato è tenuto al rispetto della normativa vigente in materia di tutela dei dati personali, di cui al Regolamento (UE) 2016/679, D. Lgs. n. 196/2003 e del D. Lgs. n. 101/2018 e a conformare il trattamento dei dati secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

- Le operazioni di trattamento devono essere eseguite esclusivamente per gli scopi inerenti l'attività svolta dal Libero Consorzio Comunale di Ragusa e nel rispetto dei principi di cui all'art. 5 del citato Regolamento.

3) DISPORRE CHE i predetti "Autorizzati al Trattamento", ciascuno per il proprio ambito e/o mansione di competenza svolta, provvedano a tutte le attività previste dalla vigente normativa in materia, dal regolamento dell'Ente, e a tutti i compiti affidatigli dal sottoscritto Sub- Responsabile interno del trattamento, ed in particolare:

- Effettuare operazioni di trattamento sotto la diretta autorità del sottoscritto Responsabile del Servizio, attenendosi alle istruzioni impartite.
- Adottare misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti contro i rischi di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- Accedere ai dati utilizzando tutte le disposizioni di sicurezza impartite, quali, a titolo esemplificativo ma non esaustivo, l'uso della ID e PW personali da non cedere ad alcuno, effettuare sui dati solo le operazioni inerenti alla propria mansione, segnalare le anomalie riscontrate.
- Non cedere ad alcun soggetto, compresi gli interessati, nemmeno in consultazione né in comunicazione né in diffusione i dati conferiti o gestiti per l'effettuazione del servizio.
- Informare il sottoscritto Sub-Responsabile interno del Trattamento, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy.

4) DARE ATTO CHE:

4.a la nomina ad incaricato non implica l'attribuzione di compiti e funzioni ulteriori rispetto a quelle già assegnate ma costituisce soltanto una autorizzazione a trattare dati personali conformemente al GDPR, alla normativa interna di adeguamento, alle Linee guida delle Autorità di controllo, alle specifiche istruzioni sulle modalità cui attenersi nel trattamento di seguito indicate e, infine, alle eventuali indicazioni del RPD/PDO.

4.b nel trattare i dati personali contenuti in documenti cartacei, l'autorizzato al trattamento è tenuto, fra l'altro, a:

- custodire con la cura necessaria, al fine di garantirne la massima riservatezza, i documenti contenenti i dati personali in un armadio o in un cassetto chiusi a chiave o comunque non accessibili alle persone non autorizzate;
- raccogliere prontamente, nel caso di stampanti di rete o fax ubicati in locali comuni (ad es. corridoi), i documenti stampati o ricevuti via fax, soprattutto se contenenti dati personali, in modo da preservarne la riservatezza dei contenuti;

- conservare con le dovute cautele le chiavi utilizzate per i cassetti e gli armadi dove sono conservati i documenti contenenti dati personali;
- prevedere opportuni meccanismi per garantire la disponibilità delle stesse anche durante periodi di assenza;
- eseguire eventuali ulteriori istruzioni che saranno comunicate all'incaricato dal Responsabile del trattamento designato dal titolare, ratione materiae, in relazione allo specifico trattamento svolto.

4.c nel trattare i dati personali con strumenti informatici, l'autorizzato al trattamento è tenuto, fra l'altro a:

- custodire con cautela le credenziali di autorizzazione per l'accesso ai locali ove previste (es. badge, chiavi, tessere identificative, ecc.);
- dare immediata comunicazione al responsabile dei sistemi informativi dell'Ente dell'eventuale smarrimento delle credenziali istituzionali;
- utilizzare la postazione di lavoro in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi;
- proteggere i computer e le altre strumentazioni informatiche, in caso di assenza, anche temporanea, dalla postazione di lavoro, tramite la sospensione o il blocco della sessione di lavoro;
- non lasciare incustoditi, anche per brevi intervalli di tempo, i dispositivi mobili e a non esportare dai locali della struttura dispositivi mobili contenenti dati personali, se non espressamente autorizzato.
- curare l'accesso ai dati trattati con strumentazioni informatiche e dovrà avvenire esclusivamente previa autenticazione. Ogni credenziale di autenticazione si riferisce ad un singolo utente. Non è consentito l'utilizzo della stessa credenziale da parte di più utenti. In particolare l'incaricato del trattamento è tenuto a custodire le proprie credenziali di accesso ai sistemi adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo, nonché ad attivarsi immediatamente in caso di furto delle credenziali. Inoltre, si precisa che la password di accesso ai dati è segreta e personale. Resta inteso che la designazione ad autorizzato ha validità per l'intera durata del rapporto di lavoro e decadrà in qualunque caso di cessazione del rapporto di lavoro con l'Ente o dietro espresso provvedimento di revoca da parte del dirigente (responsabile del trattamento), fermo restando l'obbligo di riservatezza dei dati personali e il rispetto del segreto d'ufficio cui è tenuto il dipendente.

5) ALLEGARE al presente provvedimento, per quanto sopra disposto, le "Specifiche istruzioni sul trattamento dei dati personali", Allegato A), cui attenersi nello svolgimento delle mansioni di ufficio assegnate.

6) DARE ATTO che la presente determinazione non necessita del visto di regolarità contabile in quanto non comporta riflessi diretti o indiretti sulla situazione economico finanziaria o sul patrimonio dell'Ente.

7) DISPORRE:
- la notificazione personale del presente provvedimento ai suddetti dipendenti designati quali autorizzati al trattamento dei dati;
- la pubblicazione del presente provvedimento all'albo pretorio on-line e sulla sezione Amministrazione trasparente dell'elenco dei disegnati con i relativi punti di contatto accessibili dagli interessati;
- la comunicazione della presente determinazione al DPO, di Ente e ai responsabili degli Uffici e dei Servizi ed a tutto il personale dell'Ente.

Si attesta altresì che, ai sensi ed agli effetti dell'art. 7 della L.R. 21.05.2019, n. 7, nella formazione della presente proposta di determinazione sono state valutate le condizioni di ammissibilità, i requisiti di legittimità e i presupposti ritenuti rilevanti per l'assunzione del provvedimento ed è stata eseguita la procedura prescritta dalla vigente normativa di legge e regolamentare in materia

IL DIRIGENTE DEL SETTORE 1
Dott. Raffaele Falconieri

ISTRUZIONI OPERATIVE PER I SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Il titolare del trattamento, per il tramite del sottoscritto Dirigente ed in forza del principio di «responsabilizzazione», impartisce a ciascun soggetto autorizzato sopra elencato le istruzioni a cui è obbligato ad attenersi, sotto la comminatoria delle sanzioni di legge.

DEFINIZIONI
Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR), 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.

La presente autorizzazione viene rilasciata con le seguenti istruzioni che costituiscono cogenti prescrizioni, anche ai fini della responsabilità personale:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR), 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;
- in attuazione del principio di «liceità, correttezza e trasparenza»: raccolta, registrazione, elaborazione di dati, agli esclusivi fini dell'inserimento o arricchimento degli archivi/banche dati presenti nell'Ufficio di appartenenza, nell'osservanza delle tecniche e metodologie in atto;
- in attuazione del principio di «minimizzazione dei dati»: obbligo di trattamento dei soli ed esclusivi dati personali che si rivelino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun incaricato è preposto l'incaricato;
- in attuazione del principio di «limitazione della finalità»: trattamento conforme alle finalità istituzionali del titolare e limitato esclusivamente a dette finalità;
- in attuazione del principio di «esattezza»: obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, e obbligo di verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati;

- in attuazione del principio di «limitazione della conservazione»: obbligo di conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati e obbligo di esercitare la dovuta diligenza affinché non vengano conservati, nell'Ufficio di competenza, dati personali non necessari o divenuti ormai superflui. Alla conclusione del trattamento, obbligo di assicurarsi che i documenti contenenti dati sensibili vengano conservati in contenitori/armadi muniti di serratura o in ambienti ad accesso selezionato e vigilato, fino alla restituzione;

- in attuazione del principio di «integrità e riservatezza»: obbligo di garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente ed integrale attuazione alle misure logistiche, tecniche informatiche, organizzative, procedurali definite dal titolare, trattando i dati stessi con la massima riservatezza ai fini di impedire trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;

- in attuazione del principio di «liceità, correttezza e trasparenza»: autorizzazione a comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal titolare del trattamento. Le stesse istruzioni e prescrizioni cogenti sono obbligatorie anche per il trattamento di dati personali realizzato, interamente o parzialmente, con strumenti elettronici, contenuti in archivi/banche dati o destinati a figurarvi.

In particolare, per tali trattamenti ciascun incaricato ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

- Password e username (credenziali di autenticazione informatica)

  Le credenziali di autenticazione informatica sono individuali. Non possono essere condivise con altri autorizzati al trattamento.
  La password che ciascun autorizzato imposta, con il supposto e l'assistenza, in caso di difficoltà, dell'amministratore di sistema, deve essere composta da almeno otto caratteri (di cui una lettera maiuscola, un numero e un carattere speciale), non deve essere riconducibile alla persona e deve essere cambiata ogni tre mesi a cura del soggetto.

- Logout

  Ciascun incaricato, al termine di ogni sessione di trattamento, ha l'obbligo di uscire dall'applicazione utilizzata e di effettuare il logout.

- Supporti di tipo magnetico e/o ottico

  Ciascun incaricato ha l'obbligo di:
  - verificare che i contenitori degli archivi/banche dati (armadi, cassettiere, computer, etc.) vengano chiusi a chiave e/o protetti da password in tutti i casi di allontanamento dalla postazione di lavoro;
  - evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;
  - assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le necessarie operazioni di formattazione;
  - di rivolgersi tempestivamente, per difficoltà o questione inerente la sicurezza, al sottoscritto responsabile del servizio, individuato con decreto sindacale come responsabile interno del trattamento dei dati personali.

Le principali operazioni degli incaricati 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.

Laddove si esegue il trattamento di dati personali, deve essere possibile riporre 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.

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.

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.

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

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.

Il Dirigente

IL DIRIGENTE
Dott. Raffaele Falconieri)