ISTRUZIONI OPERATIVE PER IL TRATTAMENTO DEI DATI COMUNI AL PERSONALE DIPENDENTE DEL TITOLARE O SUBINCARICATO DEI RESPONSABILI DEL TRATTAMENTO ESPRESSAMENTE NOMINATI DA MULTISERVIZI CAERITE SPA (EX. "INCARICATI DEL TRATTAMENTO"), ART. 28 REG. UE 2016/679 E DEL D. LGS 101/2018

Premessa metodologica

Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" *(si veda, in particolare, art. 4, n. 10, del regolamento)*. Nel prosieguo del documento, ai fini di una maggiore chiarezza espositiva, verranno indicati come sub-responsabili tutti quei soggetti che non rivestono la qualifica di personale dipendente del titolare o dei responsabili del trattamento, indicando invece come incaricati del trattamento tutti quei soggetti sottoposti alla potestà datoriale indipendentemente dalla forma contrattuale che rivesta in concreto il rapporto di lavoro tra le parti.

1. Glossario

Vengono di seguito riportate le definizioni dei concetti che ricorrono più spesso all'interno del presente documento. Per un'analisi più approfondita si rimanda al testo del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e al D. Lgs 101/2018, recante le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE 2016/679.

1. **Normativa sulla protezione dei dati,** si riferisce sia al regolamento Ue 679/2016 che al Decreto Legislativo italiano numero 101 del 2018.
2. **Dato personale,** sta ad indicare qualsiasi informazione che permetta l'identificazione di una persona fisica può essere direttamente o indirettamente identificata mediante il riferimento a quel dato.
3. **Categorie particolari di dati,** fa riferimento a quei dati personali relativi a: origine etnica; salute fisica e mentale (tra cui, ad esempio, dettagli di motivi per assenze per malattia in un lavoratore, ricette mediche, esami diagnostici eccetera); vita sessuale; caratteristiche genetiche; dati biometrici, se usati a scopo di identificazione; religione o convinzioni ideologiche; opinioni politiche e appartenenza sindacale; il trattamento dei dati riferibili a queste categorie particolari richiede cautele aggiuntive.
4. **Trattamento del dato,** fa riferimento alle operazioni di elaborazione comunque intese: raccolta, registrazione, detenzione, aggiunte alle informazioni i dati, qualunque operazione o insieme di operazioni che viene effettuata sui dati inclusa la cancellazione.
5. **Interessato,** fa riferimento alla persona fisica a cui i dati si riferiscono.
6. **Titolare del trattamento,** fa riferimento ad una persona fisica o giuridica che da sola o congiuntamente con altre persone fisiche determina gli scopi e le modalità in cui qualsiasi trattamento di dati personali effettuato. Nel caso della presente politica il titolare del trattamento è **Multiservizi Caerite spa con Socio Unico Comune di Cerveteri, Società soggetta all'attività di direzione e coordinamento del Comune di Cerveteri, V.lo M. Sollazzi,3 00052 Cerveteri (Rm) – CF/PI 07105121003 – REA RM 1011327**, in persona del legale rappresentante pro-tempore, o di altro soggetto appositamente designato dal legale rappresentante con propria deliberazione che abbia facoltà e poteri per agire in nome e per conto del titolare per dare riscontro alle richieste degli interessati nell'esercizio dei propri diritti garantiti dalla legge in tema di trattamento dei dati personali.
7. **Responsabile del trattamento,** fa riferimento a qualsiasi soggetto diverso da un membro del personale organico al titolare, o organizzazione che tratta dati per conto del titolare, sotto direttive dello stesso.
8. **Valutazione di impatto sulla protezione dei dati,** fa riferimento ad un processo formalizzato di valutazione dei rischi che il trattamento comporta sul libertà e i diritti dell'interessato.
9. Le espressioni **violazione della sicurezza** ovvero **data breach**, fanno riferimento a qualunque incidente, reale o potenziale, suscettibile di provocare divulgazione non autorizzata, danneggiamento distruzione o perdita di dati personali.
10. **Informativa sulla privacy,** fa riferimento ad un documento redatto per informare l'interesse della base giuridica e delle finalità del trattamento. Può essere generale o speciale per singoli trattamenti o insiemi di esse.
11. **Data Protection officer,** abbreviato in **DPO** oppure **RPD**, fa riferimento ad un professionista di

riferimento del titolare del trattamento, che lo nomina con la responsabilità principali osservare, valutare e organizzare la gestione del trattamento dei dati personali, affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

Campo di applicazione

Al fine di permettere una corretta e sicura gestione dei dati trattati a qualsiasi titolo, gli Incaricati del trattamento (di seguito "Incaricato") provvedono a rispettare le seguenti istruzioni operative, con il supporto del Titolare del trattamento (di seguito "Titolare"), del Responsabile del trattamento (di seguito "Responsabile") e del Responsabile di protezione dei dati (di seguito "RPD").

Nell'ambito dello svolgimento delle proprie mansioni, è necessario e doveroso innanzitutto fare riferimento agli obblighi riportati nell'atto di nomina con cui l'Incaricato viene autorizzato al trattamento dei dati per conto del Titolare.

L'Incaricato deve impegnarsi a:

1. trattare dati personali in conformità alle istruzioni documentate del Titolare e/o del Responsabile del trattamento;
2. adottare tutte le misure di sicurezza predisposte dal Titolare e/o dal Responsabile del trattamento;
3. assistere il Titolare e/o il Responsabile del trattamento nella predisposizione misure tecniche e organizzative adeguate a proteggere i dati personali e atte a garantire il rispetto degli obblighi previsti dal Regolamento Europeo (Artt. Da 32 a 36);
4. cancellare o restituire tutti i dati personali detenuti fuori dal luogo di lavoro al Titolare e/o al Responsabile del trattamento al termine del proprio rapporto lavorativo;
5. mettere a disposizione del Titolare e/o al Responsabile del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Regolamento Europeo;
6. collaborare alle attività di revisione, vigilanza e controllo realizzate dal Titolare e/o al Responsabile del trattamento;
7. informare immediatamente il Titolare e/o al Responsabile del trattamento qualora, a suo parere, un'istruzione violi delle disposizioni in materia di privacy.

Istruzioni operative

1. Istruzioni generali

1.1. Il trattamento dei dati personali deve avvenire da parte degli incaricati seguendo quanto riportato nel Piano di Lavoro in corso di validità ed in riferimento alle disposizioni stabilite dal Titolare e/o Responsabile;

1.2. I dati personali trattati devono essere:

1.2.1. pertinenti alla mansione da svolgere;

1.2.2. non eccedenti le necessità del lavoro;

1.2.3. corretti e tempestivamente aggiornati;

1.3. trattati in modo da ridurre al minimo i rischi:

1.3.1. di distruzione o perdita;

1.3.2. di accesso agli stessi da parte di persone non autorizzate;

1.3.3. di trattamento non autorizzato.

1.4. Gli incaricati devono:

1.4.1. nel limite del possibile, tenere chiuso a chiave il proprio ufficio, con chiave in possesso dei soli autorizzati;

1.4.2. a fronte della richiesta di conoscenza di dati personali provenienti da parte di persone diverse dall'interessato, verificare la legittimità della richiesta stessa ed eventualmente rifiutarsi di fornire i dati a chi non ne abbia il diritto.

1.5. In generale occorre:

1.5.1. non lasciare incustoditi pratiche contenenti informazioni su persone fisiche o giuridiche;

1.5.2. non lasciare incustoditi i terminali ed i dispositivi elettronici, in special modo se accessibili o visibili dall'esterno;

1.5.3. L'accesso ai locali contenenti dati personali è permesso solo alle persone autorizzate, secondo quanto riportato nel Manuale di Gestione Privacy e quanto stabilito dal Titolare e dal Responsabile;

1.5.4. È vietato commentare con colleghi e/o soggetti esterni i dati sensibili e/o giudiziari di cui si dovesse venire a conoscenza nello svolgimento del proprio lavoro;

1.5.5. L'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso.

2. Utilizzo degli strumenti elettronici

2.1. L'uso delle apparecchiature informatiche che contengono dati personali è permesso solo per svolgere le attività previste nelle istruzioni impartite agli incaricati;

2.2. L'elaboratore assegnato per lo svolgimento dei compiti d'ufficio deve essere adoperato e custodito con attenzione. Monitor e tastiera costituiscono una finestra aperta su archivi e dati: un comportamento superficiale espone al rischio di conseguenze anche penali. Pertanto si richiede di:

2.2.1. impostare l'attivazione di uno screen-saver (funzione salva schermo) con richiesta di password per ristabilire la sessione di lavoro in corso se la postazione viene lasciata incustodita durante l'orario di lavoro;

2.2.2. assicurarsi di aver spento i propri elaboratori al termine della giornata di lavoro;

2.2.3. non abbandonare la propria postazione incustodita per periodi lunghi;

2.2.4. nell'abbandonare la postazione chiudere i documenti cui si sta lavorando;

2.2.5. non lasciare la postazione collegata in rete se non c'è necessità;

2.2.6. chiudere la propria sessione di lavoro o disconnettersi ogni volta che ci si assenta;

2.2.7. evitare di prendere documenti da computer esterni, e comunque sempre verificare file e dischi provenienti da terzi.

2.3. Garantire il mantenimento delle funzioni ottimali dei sistemi elettronici contattando il responsabile della manutenzione degli strumenti elettronici:

2.3.1. prima di effettuare qualsiasi operazione incerta del risultato;

2.3.2. appena si notano disfunzioni a livello hardware, software o nei sistemi di protezione (antivirus e firewall);

2.3.3. prima di installare dispositivi hardware od applicazioni;

2.3.4. se sono stati accidentalmente scaricati virus o dialer (programmi che modificano il numero di telefono chiamato) da internet o dalla posta elettronica.

2.4. Gli incaricati autorizzati ad accedere ad internet devono utilizzare solo i servizi cui sono abilitati;

2.5. Gli incaricati non sono autorizzati a scaricare alcun tipo di software sia esso freeware o shareware senza il consenso del Titolare e/o Responsabile;

2.6. Gli incaricati devono conservare i dati sensibili in formato elettronico contenuti sui PC in maniera criptata, con password di accesso in possesso dei soli autorizzati al trattamento;

2.7. In merito alla gestione della posta elettronica, gli incaricati:

2.7.1. non devono aprire messaggi provenienti da indirizzi sconosciuti e/o con oggetto differente dall'attività che viene svolta, né gli eventuali allegati;

2.7.2. non devono inviare per posta elettronica informazioni riservate o particolarmente delicate per l'interessato senza adottare misure di protezione specifiche;

2.7.3. devono filtrare i messaggi di entrata al fine di escludere la presenza di virus;

2.8. Nel caso in cui per l'esercizio delle attività sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi USB, CD-ROM, ecc), su cui sono memorizzati dati personali, essi vanno custoditi con cura, né messi a disposizione o lasciati al libero accesso di persone non autorizzate;

2.9. I supporti rimovibili contenenti dati personali se non utilizzati vanno distrutti o ripuliti dai dati contenuti;

2.10. In caso di comunicazioni elettroniche per finalità istituzionali, queste comunicazioni vanno poste in essere seguendo le indicazioni fornite dal titolare o dal responsabile e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti.

3. Gestione autenticazione informatica (nome utente e password)

3.1. La password è un elemento fondamentale della sicurezza delle informazioni.

3.2. La password identifica in modo univoco l'utente del computer e dei servizi informatici. Inoltre permette l'accesso ad aree riservate di software, portali e siti internet utilizzati quotidianamente

per lo svolgimento delle attività oggetto dell'incarico / mansione. Non è conveniente usare una sola password per accedere a diversi servizi, poiché può compromettere la sicurezza degli account. E' bene quindi creare una password differente per ogni servizio usato.

3.3. La tendenza a condividere le password aumenta il rischio di perderne il possesso ed essere acquisite per scopi malevoli. È dunque essenziale che la password sia mantenuta riservata e non comunicata ad altri.

3.4. Per un'accorta creazione e una corretta conservazione delle password è necessario rispettare le seguenti indicazioni:

3.5. una password sicura deve essere lunga almeno 8 caratteri alfanumerici, contenere caratteri speciali (per esempio +$_^) e possedere sia minuscole che maiuscole;

3.6. la password non dovrebbe contenere parole comuni come per esempio "password" piuttosto che "qwerty" o "1234";

3.7. la password non deve essere banale o facilmente individuabile;

3.8. la password non deve coincidere con nomi propri o nomi comuni o date;

3.9. la password non deve contenere il nome utente o il proprio nome o altre informazioni personali quali il codice fiscale;

3.10. la password deve essere mantenuta riservata e non comunicata ad altri utenti. Se eccezionalmente dovesse essere necessario fornirla in caso di emergenza ad altra persona, va cambiata subito dopo;

3.11. la password non possono essere lasciate incustodite, né in libera visione, ma deve essere annotata su supporti cartacei od elettronici, a patto che non sia facilmente reperibile da altri (es. password scritta su foglio conservato in cassetto chiuso a chiave);

3.12. non è consentito usare l'opzione, che alcuni software come Internet Explorer offrono, di salvare automaticamente la password per successivi utilizzi delle applicazioni;

3.13. il periodo massimo di validità della password è di 6 mesi; dopo tale periodo è necessario sostituire la password con una nuova diversa dalla precedente;

3.14. non deve essere ripetuta una password usata in passato;

3.15. Non è consentito che due persone accedano al sistema con lo stesso identificativo utente;

3.16. Gli incaricati devono assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e sicurezza del sistema. A tal fine, è necessario prevedere un sistema che agevoli il reperimento delle password anche in assenza dell'incaricato. Tale procedura è descritta nel Manuale di Gestione Privacy, all'interno del quale viene individuato anche il soggetto responsabile del suo corretto svolgimento, il Custode della password, addetto a conservare le password utilizzate dagli incaricati in un luogo chiuso e protetto;

3.17. In caso di smarrimento e/o furto della password gli incaricati devono darne immediata notizia al Responsabile e/o al Titolare

4. Gestione dei dati in formato cartaceo

4.1. Gli archivi contenenti dati personali devono essere custoditi in modo da ridurre al minimo i rischi di perdita degli stessi e di accesso da parte di persone non autorizzate. Gli incaricati, in riferimento ai supporti cartacei contenenti dati personali, devono pertanto rispettare le seguenti indicazioni:

4.2. Mantenere i documenti cartacei ordinati e aggiornati;

4.3. Riporre i documenti, quando non sono necessari, negli appositi contenitori quali archivi, cassetti e armadi muniti di serratura ed in luoghi non direttamente accessibili a persone non autorizzate, avendo cura che le chiavi di apertura dei contenitori siano conservate in un luogo sicuro e segreto, noto solo al personale autorizzato;

4.4. Dismettere, secondo le disposizioni del responsabile, i dati personali che non sono più necessari per le finalità dell'attività;

4.5. È vietato effettuare copie fotostatiche o di qualsiasi altra natura di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento per scopi diversi da quelli autorizzati dal responsabile;

4.6. È vietato sottrarre, cancellare, distruggere, senza l'autorizzazione del responsabile, stampe, tabulati, elenchi, rubriche ed ogni altro materiale riguardante i dati oggetto del trattamento;
4.7. È vietato consegnare a persone non autorizzate stampe, tabulati, elenchi, rubriche ed ogni altro materiale riguardante i dati oggetto del trattamento.