Allegato 1 - Elenco dei Compiti ed istruzioni per il "Designato al trattamento dei dati"

PRINCIPI GENERALI DA OSSERVARE

Ogni *trattamento* di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale:

I dati devono essere trattati:

- ✓ secondo il principio di **liceità,** vale a dire conformemente alle disposizioni vigenti in materia di protezione dei dati personali, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- ✓ secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

I dati devono essere raccolti solo per **scopi**:

- ✓ **determinati,** vale a dire che non è consentita la raccolta come attività fine a se stessa;
- ✓ **espliciti**, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
- ✓ **legittimi**, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
- ✓ **compatibili** con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;

I dati devono, inoltre, essere:

- ✓ **esatti**, cioè, precisi e rispondenti al vero e, se necessario, **aggiornati**;
- ✓ **pertinenti**, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni affidate, in relazione all'attività che viene svolta;
- ✓ **completi**: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
- ✓ **non eccedenti** in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso (*c.d.* principio di minimizzazione);
- ✓ **conservati** per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

  In particolare, eventuali dati idonei a rivelare lo **stato di salute** o la **vita sessuale** sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo e, se cartacei, archiviati in cassetti o armadi con chiusura a chiave.

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di **riservatezza** e nel rispetto della dignità e della libertà dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dalla vigente disciplina in materia di protezione dei dati personali è necessario provvedere alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

La **responsabilità penale** per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

In merito alla **responsabilità civile,** si fa rinvio alla vigente disciplina in materia di protezione dei dati personali che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornire la prova di avere applicato le **misure di sicurezza adeguate** a garantire appunto la sicurezza dei dati detenuti.

Il Designato al trattamento dei dati", operando nell'ambito dei principi sopra ricordati e delle funzioni connesse al trattamento dei dati personali, deve attenersi ai seguenti **compiti di carattere particolare**:

A) collaborare e supportare il Titolare del trattamento e il Responsabile della protezione dei dati al fine di identificare e censire i **trattamenti** di dati personali (*c.d.* Registro delle Attività di Trattamento), le **banche dati** e gli **archivi** gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza, nonché collaborare con il Responsabile della Protezione dei Dati, nell'ambito delle attività affidate all'Area di competenza, nell'attività di aggiornamento del Registro delle Attività di Trattamento (di cui all'art. 30 Reg. UE 2016/679);

B) definire, per ciascun trattamento di dati personali, la **durata** del trattamento e la **cancellazione** o anonimizzazione dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

C) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita (o sia stata data) l'**informativa** ai soggetti interessati, ai sensi dell'art. 13 del Regolamento UE 2016/679 (RGPD).

D) assicurare che la **comunicazione a terzi** e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti privati.

E) adempiere agli obblighi di **sicurezza**, quali:
   - **adottare, tramite il supporto del Responsabile IT o dei tecnici amministratori di sistema,** tutte le **preventive misure di sicurezza**, ritenute **adeguate** al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

F) osservare gli adempimenti previsti in caso di **nuovi trattamenti** e **cancellazione** di trattamenti:
   - in particolare, comunicare preventivamente al Titolare ed al Responsabile della Protezione dei dati, l'inizio di ogni attività (trattamento) che deve essere oggetto di analisi dei rischi, valutazione d'impatto Privacy o di consultazione preliminare al Garante;
   - assistere il Titolare del trattamento e il Responsabile della Protezione dei Dati nel processo di valutazione d'impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment) di cui all'art. 35 del Regolamento, nonché nella eventuale fase di consultazione preventiva con l'Autorità di controllo ai sensi dell'art. 36 del Regolamento, qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio;

- segnalare al Titolare ed al Responsabile della Protezione dei dati l'eventuale cessazione di trattamento;

G) Trasmettere, per conoscenza, eventuali richieste degli interessati al **Responsabile della Protezione dei dati,** ai fini dell'esercizio dei diritti dell'interessato, ai sensi degli artt. 15-20 del RGPD e collaborare, come da procedura interna, con il Titolare del trattamento o il Responsabile della Protezione dei Dati al fine di soddisfare gli obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato e fornire tutto il supporto necessario al fine di consentire una risposta nel termine di un mese, dalla richiesta, prorogabile di due mesi nei casi di particolare complessità (ai sensi dell'art. 12, comma 3, del Regolamento).

Per quanto concerne gli archivi cartacei, l'accesso è consentito solo se previamente autorizzato dal Titolare del trattamento e deve riguardare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle funzioni assegnate del proprio settore di competenza, avendo particolare riguardo alle seguenti istruzioni:
- i documenti cartacei devono essere prelevati dagli archivi per il tempo strettamente necessario allo svolgimento dell'attività assegnata;
- atti e documenti contenenti dati sanitari devono essere custoditi in contenitori muniti di serratura e devono essere controllati in modo tale che a tali atti e documenti non possano accedere persone prive di autorizzazione. I documenti pertanto non possono essere lasciati incustoditi sulle scrivanie e in luoghi aperti al pubblico, in assenza di altri incaricati addetti al medesimo trattamento;
- atti e documenti contenenti dati sanitari devono essere riposti in luoghi custoditi e messi in sicurezza al termine delle operazioni affidate;
- qualora sia necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti" o, in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili.

Ulteriori istruzioni specifiche per il trattamento dei dati personali:

- conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in suo possesso e uso esclusivo.
- la parola chiave, quando è prevista dal sistema di autenticazione (per l'accesso al pc o ai software utilizzati), deve essere personale e composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave non deve contenere riferimenti a sé agevolmente riconducibili, deve essere modificata al primo utilizzo e, successivamente, almeno ogni tre mesi.
- non deve in nessun caso essere lasciato incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali (se ci si allontana deve essere attivata la funzione "screen saver" con password).
- occorre osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta;
- utilizzare gli strumenti informatici assegnati esclusivamente per l'esecuzione dei compiti e mansioni lavorative affidate, con espresso divieto di installare programmi software non esplicitamente autorizzati o privi di licenza;
- evitare la creazione di nuove banche dati (con finalità diverse da quelle già previste) senza espressa autorizzazione;

- svolgere operazioni di trattamento unicamente su dati/banche dati ai quali si ha legittimo accesso, nel corretto svolgimento del rapporto di lavoro e utilizzare a tal fine gli strumenti indicati o messi a disposizione dal Titolare (l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro);
- evitare di lasciare incustodito il proprio posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati o di lasciare incustoditi e accessibili a terzi gli strumenti elettronici mentre è in corso una sessione di lavoro;
- provvedere alla cancellazione o distruzione dei documenti solo su autorizzazione e con le modalità indicate dall'Amministrazione comunale;
- non comunicare via telefono o e-mail informazioni relative a terzi senza essersi accertata dell'identità del destinatario e dell'esistenza di una causa che ne legittimi la comunicazione;
- in caso si constati o si sospetti un incidente di sicurezza (ogni tentativo di violazione, illecito, errore e/o anomalia riscontrati, ecc.) dare immediata comunicazione al Responsabile IT e al Responsabile della protezione dei dati, seguendo la procedura prevista in caso di DATA BREACH.