COMUNE DI BALESTRATE
CITTA' METROPOLITANA DI PALERMO

ALLEGATO 4

PROTEZIONE DEI DATI PERSONALI E SMART WORKING

In occasione dell'avvio della sperimentazione della modalità lavorativa in *Smart Working*, si ricorda che è doveroso prestare costante attenzione alla protezione dei dati personali e adottare, in qualsiasi occasione, lavorativa e privata, un comportamento improntato alla difesa della privacy degli interessati che entrano in relazione con l'Ente.

Fermo restando quanto disposto in materia di privacy dalla normativa interna, si ritiene opportuno ricordare le principali definizioni di riferimento in materia, gli obblighi in capo ai dipendenti e le conseguenze di eventuali violazioni.

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.

Interessato: il soggetto interessato è la persona fisica che ha conferito i propri dati personali al Titolare del trattamento.

Titolare del trattamento (Comune di Balestrate): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che singolarmente o insieme ad altri, determina le finalità ed i mezzi di trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

DPO o RPD: il Data Protection Officer o Responsabile della Protezione dei Dati del Comune di Balestrate è il dott. Marco La Diega a cui è possibile fare riferimento per ricevere informazioni rispetto al trattamento dei propri dati personali e per esercitare i propri diritti di interessato. È una figura che va ad affiancare il Titolare nella gestione dei trattamenti effettuati dall'Ente ed è contattabile ai seguenti recapiti:

- n. telefono: 3345330727
- e-mail: me@marcoladiega.it
- posta certificata (pec): comunebalestrate@pec.it

Violazione dei dati personali/Data Breach: è severamente sanzionata dal Regolamento (UE) 2016/679 la violazione dei dati personali, cioè 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.

Tale violazione può afferire a una "violazione della riservatezza", in caso di divulgazione o accesso accidentale ai dati personali, a una "perdita della disponibilità", in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata), a una "violazione dell'integrità", in caso di alterazione non autorizzata o accidentale dei dati personali.

La violazione, in rapporto alla sua gravità, comporta l'obbligo di notifica del Data Breach, cioè della violazione dei dati personali al Titolare del trattamento, all'Autorità di Controllo (Garante per la protezione dei dati personali), nonché, qualora ne abbiano un danno, ai soggetti i cui dati sono stati violati.

Qualunque ipotesi di violazione dei dati personali deve pertanto essere segnalata tempestivamente al DPO che è il soggetto che informa e consiglia il Titolare o il Responsabile del trattamento da lui preposto, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento UE 2016/679 (c.d. GDPR) e dalle altre disposizioni della UE.

Smart Working

Lo *Smart Working* impone grande attenzione al tema della privacy e richiede la massima diligenza da parte del dipendente nella scelta del luogo dal quale lavorare da remoto nonché particolare attenzione verso le modalità di svolgimento dell'attività lavorativa.

In particolare, è necessario che il dipendente abbia cura di:

- non utilizzare dispositivi di memorizzazione esterna quali hard disk esterni o pendrive;
- lavorare al personal computer senza che soggetti estranei non autorizzati, compresi i familiari, possano accedere (leggere, fotografare, ecc.) alle informazioni visualizzate nel display del pc;
- custodire la password di accesso al pc usato in modo tale che resti assolutamente riservata;
- non lasciare incustoditi gli strumenti di lavoro (PC, tablet, smartphone), provvedendo, anche nel caso di allontanamento temporaneo dalla postazione, a disconnettere la sessione di lavoro bloccando l'operatività del computer ("ctrl-alt-canc");
- verificare attentamente l'identità dell'interlocutore con cui si entra in contatto a distanza;
- evitare che le conversazioni telefoniche possano essere ascoltate da persone estranee all'attività lavorativa non autorizzate a conoscere il contenuto della telefonata;

- non portare all'esterno dell'Ente, presso il luogo dove si svolge l'attività lavorativa in Smart Working, documentazione cartacea contenente dati personali, salvo casi eccezionali espressamente autorizzati dal Titolare o dal Referente del Titolare;

- ove necessario portare all'esterno dell'Ente documenti cartacei, trasportarli in cartelle recanti l'identificazione del dipendente, dell'Ente ed il recapito telefonico;

- evitare la stampa di documenti fuori dall'Ente e comunque custodire "sotto chiave" assicurando la massima riservatezza e poi distruggere l'eventuale documentazione cartacea (ad esempio stampa di file) che fosse necessario riprodurre nel luogo di svolgimento da remoto della prestazione lavorativa;

- informare tempestivamente il Titolare in caso di incidente di sicurezza (informatico o relativo a documentazione cartacea) che coinvolga dati personali e nei casi di furto o smarrimento dei supporti attraverso i quali si svolge la prestazione lavorativa.

_____

(luogo e data)

Per ricevuta, il Dipendente

_____