COMUNE DI FUCECCHIO

Città Metropolitana di Firenze

“ALL. 3”

TRATTAMENTO DEI DATI PERSONALI

PER I DIPENDENTI IN MODALITA’ DI LAVORO AGILE DEL COMUNE

TRATTAMENTO DEI DATI

Il/la lavoratore/lavoratrice agile è tenuto/a a mantenere la massima riservatezza sui dati e le informazioni di cui verrà a conoscenza nell’esecuzione della prestazione lavorativa.

Il/la lavoratore/lavoratrice agile deve pertanto adottare ogni azione o provvedimento idoneo a garantire tale riservatezza, ai

sensi delle vigenti previsioni normative in materia di trattamento dei dati personali e privacy.

Si considera rientrante nei suddetti dati e informazioni qualsiasi notizia attinente all’attività svolta dall’Amministrazione, ivi inclusi le informazioni sui suoi beni e sul personale, o dati e informazioni relativi a terzi in possesso dell’Amministrazione per lo svolgimento del suo ruolo istituzionale.

I dati personali devono essere trattati nel rispetto della riservatezza e degli altri fondamentali diritti riconosciuti all’interessato dalle norme giuridiche in materia di protezione dei dati personali di cui al Regolamento UE 679/2016 – GDPR e al D. Lgs. n. 196/2003 e successive modifiche – Codice Privacy. Il trattamento dovrà essere realizzato in osservanza della normativa nazionale vigente, del Regolamento UE sulla Protezione dei Dati Personali e delle apposite prescrizioni e istruzioni impartite dall’Amministrazione in qualità di Titolare del Trattamento.

ISTRUZIONI

Il/la lavoratore/lavoratrice agile è tenuto a custodire con diligenza la documentazione utilizzata, i dati e gli strumenti tecnologici eventualmente messi a disposizione dall'Amministrazione.

La prestazione lavorativa in modalità agile può prevedere l'utilizzo di documentazione cartacea istituzionale. È dovere del lavoratore utilizzare, ove possibile, modalità alternative (es. copie digitali, scansioni, ecc.) per la fruizione della documentazione affinché fuoriesca dalla sede lavorativa il minor numero di documenti cartacei. Nell'impossibilità di ciò, sarà cura del Dipendente garantire l'integrità della documentazione movimentata, la corretta custodia, la tutela e la riservatezza dei dati ivi contenuti.

Il lavoratore dovrà osservare, in particolare, le seguenti istruzioni e misure di sicurezza:

- dovrà porre ogni cura per evitare che i dati possano entrare nella disponibilità di persone non autorizzate presenti nel luogo di prestazione fuori sede; -
- individuare in casa una stanza o comunque uno spazio deputato per allestire la postazione lavorativa che possa essere utilizzato in modo, per quanto possibile, esclusivo interdicendone l'accesso agli altri familiari, con possibilità di chiusura della porta a chiave, con armadietti dotati di serratura ove riporre la documentazione e/o gli strumenti di lavoro;
- qualora, eccezionalmente, al termine del lavoro risulti necessario trattenere, presso il domicilio, materiale cartaceo contenente dati personali, lo stesso dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura;
- dovrà custodire con diligenza la documentazione, i dati e le informazioni dell'Amministrazione utilizzati in connessione con la prestazione lavorativa;
-non dovrà utilizzare dispositivi personali laddove non autorizzati direttamente dal proprio responsabile;
-qualora non si utilizzino dispositivi forniti dal titolare del trattamento, dovrà richiedere al responsabile l'installazione dell'antivirus;
- dovrà configurare la modalità di blocco automatico quando si allontani dalla postazione di lavoro;
- dovrà procedere a bloccare manualmente il dispositivo (computer, cellulare, etc) in dotazione in caso di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo;
- utilizzare il dispositivo assegnato solo ed esclusivamente per le attività lavorative evitando di utilizzarlo per accedere a social network o a qualsiasi sito web o server mail diversi da quelli necessari allo svolgimento della prestazione;
- non dovrà cliccare su link o allegati contenuti in e-mail sospette;
- dovrà effettuare sempre il log-out dai servizi/portali utilizzati dopo che si sia concluso la sessione lavorativa;
- in caso di databreach (perdita di dati), dovrà immediatamente informare il Titolare del trattamento;

- dovrà utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette;
- dovrà collegarsi esclusivamente a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui si conosca la provenienza (forniti dall'Amministrazione di appartenenza);
- non dovrà conservare file personali sui dispositivi forniti;
- dovrà evitare di rivelare informazioni di carattere personale al telefono o attraverso dispositivi dell'Ente o in videochiamata;
- dovrà evitare il collegamento a reti non sicure o sulle quali non si abbiano adeguate garanzie;
- dovrà variare le password di accesso all'utente server/posta elettronica con maggiore frequenza (ogni 3 mesi);
- assicurarsi che la postazione scelta non possa essere investita da acqua, fuoco, vento, calore eccessivo;
- con cadenza semestrale, dall'inizio dello smart working, dovrà procedere alla modifica della password del wifi della adsl (o router del telefono).

Per l'utilizzo di risorse e strumenti risorse personali, si segnala inoltre quanto segue:

- dovrà assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura;
- evitare di salvare le password di accesso ai dati sul browser o su supporti facilmente accessibili a terzi;
- dovrà utilizzare i sistemi operativi per i quali attualmente è garantito il supporto;
- dovrà effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo utilizzato;
- dovrà assicurarsi che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati;
- dovrà non installare software proveniente da fonti non ufficiali.