Allegato sub 4

Protezione dei dati personali e Smart Working

Nell'ambito della modalità di erogazione della prestazione lavorativa in Smart Working denominata "Lavoro Agile" disciplinata dalla Legge n. 81/2017 – Capo II, si ricorda che è necessario prestare costante attenzione alla protezione dei dati personali e adottare, in qualsiasi occasione, lavorativa e privata, un comportamento improntato alla difesa della privacy delle persone fisiche che entrano in relazione con l'Ente.
A tal fine si richiamano i contenuti delle informazioni fornite ai dipendenti ai sensi dell'art.13 del Regolamento dell'Unione Europea 679/2016 del 27 aprile 2016 (GDPR), le norme vigenti per il trattamento dei dati personali e "categorie particolari di dati personali" dei dipendenti e le Policy interne in materia, con le obbligazioni ivi riportate a carico dei singoli dipendenti in relazione al ruolo ricoperto nell'organizzazione privacy dell'Ente e in ottemperanza al principio dell'accountability (responsabilizzazione) previsto dal Regolamento sopra citato.
Ferme restando le prescrizioni in materia di privacy dell'Ente, si ritiene necessario fornire alcune definizioni e approfondimenti in materia di privacy, per esempio che cosa si intenda per "dato personale" e "trattamento", quali siano i soggetti coinvolti e che cosa comporti una violazione dei dati personali "Data Breach".
Inoltre si riporta di seguito il "Decalogo Privacy "Lavoro Agile", finalizzato a orientare gli atteggiamenti e i comportamenti dei Lavoratori che aderiscono al "Lavoro Agile".

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.

Titolare del trattamento (ALFA): 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.

Responsabile della protezione dei dati: Responsabile della Protezione dei Dati (RPD o Data Protection Officer), nominato dal Titolare del trattamento ai sensi dell'Articolo 37 del Regolamento Generale sulla protezione dei dati, nella persona giuridica di Liguria Digitale S.p.A. Il RPD è il soggetto che informa e consiglia il Titolare o il Responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento UE 2016/679 (c.d. GDPR) e dalle altre disposizioni della UE.

Violazione dei dati personali/Data Breach
I dati personali conservati, trasmessi o trattati possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti, perdita o furto di dispositivi informatici. Si tratta di situazioni che possono comportare pericoli significativi per la privacy delle persone fisiche a cui si riferiscono i dati.
Per questo motivo si rende necessaria una maggiore attenzione da parte dell'Ente nel predisporre misure tecniche e organizzative adeguate che garantiscano la tutela dei dati personali e prevengano la violazione dei dati personali "Data Breach", 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, alla "perdita della disponibilità", in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata) e alla "violazione dell'integrità", in caso di alterazione non autorizzata o accidentale dei dati personali.
La violazione, in rapporto alla sua gravità, può comportare per il Titolare del trattamento (ALFA) la notifica del Data Breach all'Autorità di Controllo (Garante per la protezione dei dati personali), nonché, qualora ne abbiano un danno, la comunicazione agli interessati i cui dati sono stati violati.
Qualunque presunta o sospetta violazione dei dati personali deve essere segnalata tempestivamente all'indirizzo mail dpo.privacy@alfaliguria.it. Si ricorda che è severamente sanzionata dal Regolamento (UE) 2016/679 la mancata notifica di violazione dei dati personali all'Autorità di Controllo e la comunicazione agli interessati, qualora siano necessarie.

"Decalogo privacy Lavoro Agile"
Il "lavoro Agile" impone la massima attenzione sui temi della riservatezza e presuppone che il dipendente rimanga sempre concentrato sulle modalità di lavoro (in parte all'interno dei locali aziendali e in parte all'esterno senza una postazione fissa) in modo corretto ed idoneo per proteggere l'operatività e la reputazione dell'Ente.
Le conversazioni tra il dipendente e gli altri interessati non devono essere oggetto di ascolto da parte di soggetti non autorizzati, i quali devono essere mantenuti ad una distanza che consenta di proteggere la confidenzialità. Pertanto è obbligo del dipendente:

- Evitare di effettuare colloqui ad alta voce, di persona o per telefono, in presenza di soggetti non autorizzati a conoscere il contenuto della conversazione;

- Accertarsi che il coniuge o eventuali parenti e conoscenti non siano portati, anche involontariamente, a conoscenza di informazioni e processi attinenti l'attività lavorativa;

- Non utilizzare familiari o terzi per veicolare informazioni, anche se ritenute "banali", afferenti l'attività lavorativa;

- Nel caso di conversazioni telefoniche instaurate in seguito di chiamate inoltrate o ricevute, accertare, con cura, che l'interlocutore sia effettivamente un collega/cliente/fornitore legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione;

- Prestare particolare attenzione quando si trasportano da un locale all'altro, da uno stabile all'altro, da un luogo ad un altro (mediante mezzi pubblici o privati o anche a piedi) documenti contenenti dati personali. Il "Lavoro Agile" non dovrà essere effettuato, a tal fine, di norma, al di fuori di ambienti privati protetti, che garantiscano la necessaria riservatezza della prestazione.

Le cartelle di lavoro approvate dall'Azienda sono esclusivamente quelle impostate sulla rete informatica di ALFA. Non è approvato, pertanto, salvare documenti di lavoro sul proprio PC, se non occasionalmente e temporaneamente.
Più in dettaglio per quanto concerne l'utilizzo di documenti cartacei contenti dati personali e prelevati dagli archivi dell'Ente, si sottolinea che il trasferimento di dati personali deve essere giustificato da necessità strettamente correlate all'esercizio dell'attività lavorativa, agli obblighi di legge o alla difesa degli interessi dell'Ente. La circolazione dei dati personali cartacei, in situazione di mobilità deve essere ridotta al minimo indispensabile.
In particolare i documenti cartacei:
• devono essere utilizzati solo per il tempo necessario allo svolgimento dei compiti assegnati e poi ripartiti negli archivi dedicati alla loro conservazione;
• non devono essere lasciati incustoditi; pertanto, nel caso di assenza, anche momentanea, dal luogo in cui si svolge "Lavoro Agile" è necessario chiudere a chiave i locali che ospitano i dati ovvero riporli dentro un armadio/cassetto chiuso a chiave; non devono restare, senza ragione, applicati su supporti (lavagne o simili) che possono essere visionati da persone non autorizzate;

• devono essere resi illeggibili prima di essere cestinati, qualora siano destinati a divenire rifiuti (ad es. strappando più volte la carta in modo che i contenuti diventino non decifrabili/non ricostruibili);
Per quanto riguarda il trattamento di dati personali mediante l'ausilio di strumenti elettronici, si richiamano le indicazioni contenute nel Regolamento sull'Utilizzo del Sistema Informativo e si ribadisce quanto segue:

- La password di accesso deve essere conservata con diligenza in modo che resti riservata, evitando sotto la responsabilità del dipendente, che altri ne vengano a conoscenza;

- Il computer ed altri eventuali strumenti in dotazione (P.C., smartphone, ecc.) e/o utilizzati per l'espletamento delle prestazioni di "Lavoro Agile", non devono essere lasciati incustoditi ed accessibili a persone non autorizzate. In caso di allontanamento anche temporaneo dalla postazione di lavoro il dipendente è tenuto a disconnettere la sessione di lavoro bloccando l'operatività del computer ("ctrl-alt-canc") e/o l'accesso allo smartphone (password di blocco schermo).

- Non devono essere utilizzati dispositivi di memorizzazione esterna: come sopra riportato la documentazione inerente all'attività lavorativa dovrà risiedere esclusivamente sulle cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al regolamento.

Nell'ambito delle proprie attività e in osservanza alle misure derivanti dal sistema procedurale, gestionale e tecnico instaurato dall'Azienda per garantire la sicurezza dei dati personali, il dipendente tratta dati:

- Esatti e, se necessario, aggiornati;
- Archiviati in una forma che consenta l'esercizio dei diritti da parte dell'interessato di cui al Capo III del Regolamento Europeo;
- Conservati in modo tale da consentire 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;
- Ove necessario e compatibile, anonimizzati, pseudonimizzati o cifrati.

Il dipendente dovrà, altresì, adottare le cautele previste per legge (diritto all'oscuramento e anonimato) nell'eventuale trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitù; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari).
E' obbligazione contrattuale del/della dipendente rispettare dette istruzioni e partecipare alle attività formative previste dall'Azienda in punto.
Il/La dipendente è consapevole e accetta che Alfa verifichi il rispetto delle misure di sicurezza informatiche ed operative che sono state indicate all'atto di autorizzazione alla modalità operativa dello smart working, in ossequio delle previsioni della normativa vigente in materia e dell'art. 4 della L. 300/70 e s.m.i.

Data

Per ricevuta del lavoratore