LINEE GUIDA SUL TRATTAMENTO DEI DATI PERSONALI IN MODALITÀ DI "LAVORO AGILE"

Il lavoratore che svolge la propria prestazione nella modalità di lavoro agile deve, nel rispetto dell'art. 22, c. 1, l. 22 maggio 2017 n. 81, del GDPR e del D.lgs. 30 giugno 2003 n. 196 e delle raccomandazioni elaborate dall'Agenzia per l'Italia Digitale, sulla base delle misure minime di sicurezza informatica per le pubbliche amministrazioni fissate dalla circolare 17 marzo 2017, n. 1/2017, nell'assolvimento dei compiti assegnati:

- ✓ effettuare il trattamento dei dati in modo lecito e corretto;
- ✓ i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- ✓ è necessaria la verifica costante dei dati raccolti ed il loro aggiornamento.

Il lavoratore che effettua la propria prestazione lavorativa in modalità di lavoro agile:

- ✓ non può eseguire operazioni di trattamento per finalità non previste tra i compiti a lui assegnati; analogamente, le operazioni di trattamento potranno essere effettuate unicamente sui dati sui quali si è autorizzati all'accesso, nel corretto svolgimento dei compiti cui si è preposti;
- ✓ l'accesso ai dati personali deve essere limitato esclusivamente ai dati che sono strettamente necessari per adempiere ai compiti assegnati;
- ✓ l'uso delle apparecchiature informatiche in tale ambito è permesso solo per svolgere le attività previste nelle presenti istruzioni.

❖ RISERVATEZZA

Il lavoratore in modalità di lavoro agile dovrà operare garantendo la massima riservatezza delle informazioni di cui viene in possesso, considerando i dati personali oggetto dell'ambito di attività assegnate come informazioni da gestire con cura attenendosi alle seguenti prescrizioni:

- ✓ astenersi dal comunicare i dati personali a soggetti diversi da quelli indicati dal titolare e/o responsabile o che non abbiamo motivo di acquisire tali dati per il corretto espletamento dei propri compiti;
- ✓ verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, e comunque nel rispetto delle prescrizioni impartite dal titolare;
- ✓ trasmettere immediatamente al titolare del trattamento dei dati qualsiasi richiesta proveniente dagli interessati che faccia riferimento ai diritti sanciti dall'art. 15 all'art. 21 della normativa UE 2016/679;
- ✓ provvedere, quando richiesto, al rilascio dell'informativa di legge e alla raccolta ed archiviazione del relativo consenso.

Il lavoratore in modalità di lavoro agile dovrà altresì porre in essere ogni attività necessaria ad evitare i rischi di perdita o distruzione, anche accidentale, dei dati, nonché di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità per cui i dati sono stati raccolti;

- ✓ resta inteso che il lavoratore in modalità di lavoro agile è autorizzato al trattamento dei soli dati per cui è autorizzato all'accesso, in coerenza con i compiti assegnati, l'accesso a tali dati personali deve essere limitato esclusivamente a quelli strettamente necessari per adempiere ai compiti assegnati;
- ✓ l'uso delle apparecchiature informatiche e dei software aziendali in tale ambito è permesso solo per svolgere le attività previste nelle presenti istruzioni ricevute.

L'eventuale aggiornamento dei trattamenti potrà essere comunicato a parte, di volta in volta, dal titolare.

❖ PROFILO DI AUTORIZZAZIONE

Relativamente al profilo di autorizzazione per l'accesso ai sistemi informatici e ai dati, le procedure adottate sono organizzate nel rispetto del principio della separazione dei compiti, perciò sono state disegnate e attivate in modo che un soggetto non abbia compiti o responsabilità operative che risultino incompatibili fra di loro e seguendo il principio del minimo privilegio per l'accesso ai dati.

A.O.R.N. "Azienda Ospedaliera dei Colli" - Via L. Bianchi s.n.c. - 80131- Napoli
Centralino 081/7061111 – C.F./P.I. 06798201213

Il lavoratore in modalità di lavoro agile è autorizzato, nell'espletamento delle attività connesse alla funzioni amministrative, all'accesso e al trattamento di dati personali nella misura e nei limiti del GDPR e del D.lgs. 30 giugno 2003 n. 196. Inoltre, lo stesso è autorizzato, limitatamente a quanto strettamente necessario nello svolgimento della prestazione lavorativa in modalità di lavoro agile, all'accesso e al trattamento dei dati personali in occasione della gestione delle comunicazioni telefoniche e a mezzo fax. Si raccomanda al lavoratore di evitare, ove possibile, la duplicazione su qualsiasi supporto informatico o cartaceo e il trasporto di eventuali documenti e/o il trasferimento fra la propria abitazione e l'ufficio di documenti ed elenchi contenenti dati personali e dati particolari e giudiziari, nei limiti dei trattamenti consentiti dal Regolamento UE 2016/679.

❖ REGOLE DI ORDINARIA DILIGENZA

Nell'esecuzione dei compiti assegnati, il lavoratore in modalità di lavoro agile deve attenersi ad alcune regole di ordinaria diligenza al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento. In particolare:

- ✓ qualora il lavoratore abbandoni temporaneamente la propria postazione di lavoro, deve provvedere a:
  - non far accedere ai non addetti ai lavori – anche familiari - ai luoghi in cui siano presenti informazioni riservate o dati personali;
  - riporre nei cassetti o negli armadi, con chiusura dotata di serratura, la documentazione cartacea eventualmente in possesso e contenente dati personali;
- ✓ se è necessario allontanarsi dal device utilizzato in presenza anche di soli familiari, riporre i documenti e attivare il salva schermo del computer con password;
- ✓ non rivelare o far digitare password dal personale di assistenza tecnica;
- ✓ non rivelare le password al telefono, né inviarle via fax;
- ✓ accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- ✓ non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione;
- ✓ non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
- ✓ accertarsi della corretta funzionalità dei meccanismi di chiusura di armadi o cassetti, nel caso in cui occorra riporre documentazione cartacea;
- ✓ conservare e/o consegnare i documenti contenenti dati personali in modo da garantirne la riservatezza;
- ✓ provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati;
- ✓ non abbandonare la postazione di lavoro senza aver provveduto a custodire in luogo sicuro i documenti trattati.

❖ MISURE DI SICUREZZA

Il personale aziendale che opera in modalità di lavoro agile o "smartworking" potrebbe essere dotato di dispositivi appositamente predisposti, con applicativi pronti per la fruizione remota, e/o dispositivi telefonici virtuali (su software) adeguati allo scopo, o potrebbe utilizzare dispositivi propri.

In ogni caso, tutto il personale che opera in modalità di lavoro agile vedrà predisposto sul proprio dispositivo (o "device") una Virtual Private Network ("VPN"), o un equivalente canale di comunicazione "sicuro" tra il dispositivo remoto e la struttura aziendale, attraverso cui accedere direttamente agli applicativi ed ai dati aziendali.

Maggior responsabilizzazione è, quindi, richiesta a tutto il personale che opera in modalità di lavoro agile, dati i conseguenti maggiori rischi informatici che possono derivare dallo stesso.

In contesti di lavoro in ambienti domestici, di trasferta, in mobilità, o in qualsiasi altro contesto esterno all'azienda, tutto il personale dovrà rispettare le seguenti indicazioni:

- ✓ tutelare il knowhow aziendale e proteggere i dati personali trattati dal Titolare;
- ✓ seguire prioritariamente le policy e le raccomandazioni dettate dal Titolare del trattamento;
- ✓ cooperare all'attuazione delle misure di prevenzione predisposte dal datore di lavoro per fronteggiare i rischi connessi all'esecuzione della prestazione all'esterno dei locali aziendali;
- ✓ utilizzare i sistemi operativi per i quali attualmente è garantito il supporto;
- ✓ effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo;
- ✓ evitare l'uso di social network e/o altre applicazioni di carattere social che possono rendere più agevole l'intrusione esterno sul dispositivo aziendale;
- ✓ assicurarsi che i software di protezione del sistema operativo (firewall, antivirus, etc.) siano abilitati e costantemente aggiornati;
- ✓ assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dal Titolare;
- ✓ adoperare misure organizzative e di sicurezza adeguate nell'utilizzo dei dispositivi propri o aziendali, che impediscano la visuale dei non addetti ai lavori, anche in un contesto familiare per l'autorizzato, per scopi di riservatezza e di circolazione dei dati;
- ✓ non installare software proveniente da fonti/repository non ufficiali;
- ✓ non cliccare su link o allegati contenuti in email sospette;
- ✓ utilizza per l'accesso a connessioni Wi-Fi adeguatamente protette;
- ✓ utilizzare correttamente le attrezzature di lavoro, i mezzi di trasporto, nonché i dispositivi di sicurezza;
- ✓ collegarsi a dispositivi mobili (pen-drive, HDD-esterno, etc.) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dal Titolare);
- ✓ effettuare sempre il log-out dai servizi/portali utilizzati dopo che si conclude la sessione lavorativa;
- ✓ segnalare immediatamente al datore di lavoro o al dirigente le deficienze dei mezzi e dei dispositivi propri o aziendali (eventualmente ricevuti come attrezzatura per il lavoro in modalità agile);
- ✓ partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;
- ✓ evitare di rivelare al telefono informazioni aziendali e altri dati personali trattati dal Titolare;
- ✓ evitare il collegamento a reti non sicure o sulle quali non si abbiano adeguate garanzie (es. reti pubbliche);
- ✓ evitare di lasciare i dispositivi utilizzati incustoditi in luoghi di facile accesso al pubblico o ai propri familiari;
- ✓ bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro;
- ✓ il lavoratore in modalità di lavoro agile è tenuto a fornire la propria prestazione non lasciando mai incustodito lo strumento elettronico proprio o fornito dal datore attraverso il quale opera, nel caso di allontanamento occorrerà chiudere a chiave la porta della stanza ove svolge la propria prestazione lavorativa.

Scegliere una password con le seguenti caratteristiche:

- ✓ originale, composta da almeno 10 caratteri, che contenga almeno un numero, una lettera maiuscola, una lettera minuscola o un carattere speciale (almeno tre dei citati carattere), che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili curare la conservazione della propria password ed evitare di comunicarla ad altri;
- ✓ modificare periodicamente (almeno una volta ogni tre mesi) la propria password;
- ✓ modificare prontamente (ove possibile) la password assegnata dall'amministratore di sistema.

Le presenti "Linee Guida" sono pubblicate sul sito istituzionale http://www.ospedalideicolli.it/privacy/.