ASP AGRIGENTO
AZIENDA SANITARIA PROVINCIALE

Servizio Sanitario Nazionale – Regione Sicilia
AZIENDA SANITARIA PROVINCIALE AGRIGENTO
Direzione Generale- Ufficio Protezione dei Dati
Viale Della Vittoria n. 321, Agrigento 92100 - Tel. 0922/407111

ISTRUZIONI DI LAVORO DA OSSERVARE DURANTE LE SESSIONI DI SMART WORKING ("LAVORO AGILE") NEL CONTESTO EMERGENZIALE DOVUTO ALLA DIFFUSIONE DEL CORONA VIRUS

Viste le prescrizioni di cui all'art. 1 n°6) del **DPCM 11 marzo 2020** che in tema di "lavoro agile" recitano:

"Fermo restando quanto disposto dall'art. 1, comma 1, lettera e), del decreto del Presidente del Consiglio dei Ministri dell'8 marzo 2020 e fatte salve le attività' strettamente funzionali alla gestione dell'emergenza, le pubbliche amministrazioni, assicurano lo svolgimento in via ordinaria delle prestazioni lavorative in forma agile del proprio personale dipendente, anche in deroga agli accordi individuali e agli obblighi informativi di cui agli articoli da 18 a 23 della legge 22 maggio 2017, n. 81 e individuano le attività indifferibili da rendere in presenza",

Si forniscono specifiche istruzioni volte a garantire la correttezza del trattamento dei dati effettuato durante le sessioni di lavoro in smart working.

ISTRUZIONI SPECIFICHE SUL TRATTAMENTO DEI DATI

Si rammenta quanto disposto dall'art. 5 del Regolamento UE 2016/679. I dati personali oggetto di trattamento devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità …;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati …;

- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Inoltre si richiama particolare attenzione ai seguenti punti, aventi specifica attinenza con la sicurezza dei dati trattati durante le sessioni remote:

- Il trattamento dei dati **è consentito nell'ambito delle funzioni svolte**, in costanza dell'espletamento dell'incarico attribuito e solo per quelli attinenti alla propria U.O. o area di riferimento;
- **Si deve osservare cautela in qualsiasi trattamento effettuato su dati personali**;
- **E' permesso il trattamento esclusivo dei dati necessari all'attività lavorativa**, astenendosi dal trattare i dati eccedenti le finalità;
- E' indispensabile garantire **la riservatezza della documentazione** trattata e la **sicurezza dei supporti personali o messi a disposizione dall'ente**.

Inoltre occorrerà osservare scrupolosamente tutte le misure di sicurezza già in atto e quelle che saranno successivamente adottate dal titolare, nonché ogni ulteriore istruzione che sarà impartita in relazione a determinati trattamenti.

Infine si fa presente che tutte le disposizioni di futura emanazione correttive od integrative della normativa attualmente vigente in materia di protezione dei dati personali devono essere scrupolosamente osservate.

Le presenti indicazioni sono tassative.

UTILIZZO DEI SUPPORTI E DEGLI STRUMENTI DI LAVORO

Documenti e supporti, analogici e digitali

- Verificare sempre che la documentazione cartacea presa in carico venga adeguatamente registrata al momento dell'uscita dalla sede dell'Ente, così come venga adeguatamente tracciata la sua restituzione.
- In caso di consultazione di documenti cartacei in luoghi in cui sono presenti altri soggetti (questo è una cautela valida anche quando l'attività lavorativa viene svolta in ambiente domestico), prestare sempre attenzione affinché non possano essere lette, neanche accidentalmente, le informazioni ivi contenute. Non devono essere mostrati in chiaro eventuali nomi presenti su documenti o fascicoli che li contengano.

- Limitare il download dei documenti ai soli casi strettamente necessari. Eliminare dal proprio strumento informatico utilizzato, i file custoditi in locale durante le varie fasi del lavoro agile.

STRUMENTI DI ELABORAZIONE

Misure Minime di Sicurezza

Per prevenire eventuali danneggiamenti al patrimonio informativo dell'Azienda, è condizione fondamentale che l'hardware utilizzato per la connessione in VPN abbia i seguenti requisiti minimi:

- **Presenza di antivirus aggiornato;**
- **Browser aggiornato;**
- **Utilizzo di sistema operativo aggiornato e ancora supportato**

Criteri fondamentali di Sicurezza

- Non lasciare incustoditi o accessibili a terzi non autorizzati la postazione di lavoro e gli strumenti elettronici mentre è in corso una sessione di lavoro.
- Qualora un tecnico richieda di collegarsi alla postazione di lavoro tramite strumenti di controllo remoto, è indispensabile
    - verificare l'identità dell'operatore remoto (tramite conoscenza diretta o comunicazione preventiva)
    - controllare se è autorizzato allo svolgimento dell'intervento (tramite preventiva apertura di ticket, autorizzazione, …)
    - presidiare la postazione durante l'intervento, a meno che non sia stato concordato diversamente.

Credenziali di Accesso

- **Conservare la password in un luogo sicuro;**
- **Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;**
- **Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.**

Gli assegnatari degli accessi sono responsabili personalmente del corretto utilizzo degli stessi.

Sono vietati tutti gli utilizzi di detto strumento non conformi agli scopi dell'Azienda.

L'utente si impegna:

- a non modificare, senza il consenso dei Sistemi Informativi, la configurazione hardware e software della/e macchine a cui si collega;
- a non utilizzare il nome utente e la password di altri utenti;
- Al termine di ogni sessione di lavoro in cui vengono inserite le credenziali di accesso, a scollegarsi (logout) dall'applicazione e dalla connessione VPN per evitare che un altro utilizzatore usi il servizio rimasto attivo
- A informare il *Responsabile dei sistemi informativi aziendali*, nel caso in cui abbia il sospetto che la password non sia più riservata.

Posta Elettronica

Per quanto già illustrato e condiviso con il personale dipendente, si sottolinea l'importanza della corretta gestione della **casella di posta elettronica istituzionale che rimane l'unica riconosciuta dall'Azienda** quale strumento di lavoro.

Nell'ipotesi in cui l'email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato;
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;
- nel caso di invii a più destinatari, gli stessi debbano essere messi nel campo "ccn".

RAPPORTO CON SOGGETTI TERZI

- Prima di rilasciare documenti, dati o credenziali a soggetti terzi, verificare l'identità dei destinatari e la presenza di adeguate autorizzazioni al rilascio.
- Comunicare e/o diffondere solo i dati personali preventivamente autorizzati dal Titolare.
- In caso di richieste di informazioni o documenti confrontarsi prontamente con il referente del Titolare sul da farsi.

INCIDENTI DI SICUREZZA

Qualora si riscontri un incidente di sicurezza sulle risorse informative o sugli strumenti dati in dotazione dal Titolare, che possa o meno sfociare in una violazione da notificare all'autorità Garante della Privacy, è necessario comunicarlo immediatamente al referente del Titolare, al fine di allestire prontamente adeguate misure di mitigazione del danno.

INTERVENTI DI EMERGENZA CHE NECESSITINO L'UTILIZZO DI CREDENZIALI DELL'INCARICATO

In caso di necessità che renda indispensabile e indifferibile intervenire con le credenziali assegnate, per esclusive necessità di garantire la continuità dei servizi e/o la sicurezza dei dati, potrà essere consentito ad un soggetto specificamente designato l'accesso ai dati ed agli strumenti informatici, tramite modifica delle password dell'utente. Non appena possibile il personale espressamente designato dal Titolare provvederà ad informare l'assegnatario delle credenziali dell'avvenuta procedura. Al suo rientro questi dovrà obbligatoriamente provvedere ad impostare nuove password di accesso.

CONCLUSIONE DELLO STATO DI EMERGENZA

Terminata la fase di emergenza dovuta alla diffusione del Covid-19, le attività di "lavoro agile" saranno interrotte per essere, laddove previsto, ricondotte nell'alveo della conformità legislativa. Per tanto non avranno più efficacia le attività in deroga.

Luogo, data _____

Per presa visione _____