SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Parma

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

(ai sensi dell'art. 13 del Regolamento UE 2016/679)

LAVORO AGILE
("*SMART WORKING*")

Gentile dipendente/collaboratore,

in applicazione delle misure di contrasto e contenimento del diffondersi del virus COVID-19, l'Azienda, al fine di contemperare l'interesse della salute pubblica con quello della continuità delle attività istituzionali, assicura modalità di svolgimento della prestazione lavorativa in forma agile ("*smart working*") quale strumento ordinario, per il tempo dell'emergenza, anche in deroga agli adempimenti di cui agli artt. da 18 a 23 della legge 22 maggio 2017, n. 81.
Le presenti informazioni integrano le informazioni sul trattamento dei dati personali per l'instaurazione, gestione ed estinzione del rapporto di lavoro alle quali si fa rinvio.

TITOLARE DEL TRATTAMENTO E RESPONSABILE DELLA PROTEZIONE DEI DATI
Il Titolare del trattamento dei dati è l'Azienda Ospedaliero-Universitaria di Parma, con sede in Via Gramsci, 14 – 43126 Parma.
Il Responsabile della Protezione dei Dati può essere contattato all'indirizzo e-mail dpo@ao.pr.it o all'indirizzo del titolare.

FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO
I dati personali conferiti, incluso il numero personale di contatto telefonico, sono trattati esclusivamente per finalità di riorganizzazione delle modalità di svolgimento della prestazione lavorativa secondo le forme del lavoro agile, in virtù dei provvedimenti straordinari di contenimento dell'emergenza epidemiologica.
La base giuridica che conferisce liceità alle operazioni di trattamento è l'esecuzione del contratto di lavoro.

COMUNICAZIONE E PERIODO DI CONSERVAZIONE
I dati personali conferiti per l'attivazione della modalità di lavoro agile non sono oggetto di comunicazione ad altri soggetti e sono trattati da personale autorizzato per gli adempimenti di competenza (autorizzazioni, configurazioni informatiche, rendicontazioni, ecc.).
I Suoi dati sono conservati non oltre sessanta giorni successivi alla conclusione del periodo di emergenza, fatto salvo il maggior tempo necessario per adempiere ad obblighi di legge o per motivi di interesse pubblico o per l'esercizio di pubblici poteri, tenuto altresì conto di quanto previsto dal Piano di conservazione della documentazione aziendale (cd. massimario di scarto).

ESERCIZIO DEI DIRITTI
Lei può in ogni momento esercitare il diritto di ottenere: la conferma che sia o meno in corso un trattamento di dati personali che la riguardano e, nel caso, ottenere l'accesso ai dati personali; la rettifica di dati inesatti e l'integrazione di dati incompleti. Nei soli casi previsti dalla legge, ha altresì il diritto di ottenere: la cancellazione dei dati; la limitazione del trattamento; l'opposizione al trattamento.
Se ritiene che il trattamento dei Suoi dati personali sia effettuato in violazione di legge, ha il diritto di proporre reclamo al Garante per la protezione dei dati personali.

Ulteriori informazioni riguardanti il trattamento dei dati personali, incluse le modalità per l'esercizio dei diritti, sono consultabili sul sito istituzionale dell'Azienda Ospedaliero-Universitaria di Parma: www.ao.pr.it - sezione "Privacy"

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Parma

SMARTWORKING: PRINCIPALI INDICAZIONI PER LA SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI

In aggiunta alle istruzioni operative già impartite in ordine al corretto e sicuro trattamento dei dati in occasione dello svolgimento dell'attività lavorativa (vd. "*Manuale ad uso degli autorizzati*" e "*Regolamento per l'utilizzo dei sistemi informatici*" reperibili sulla intranet aziendale), l'Azienda, in qualità di titolare del trattamento, fornisce agli autorizzati le seguenti ulteriori istruzioni al fine di garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati effettuato, in modalità straordinaria "*smart working*", mediante l'utilizzo di dispositivi personali (PC/Tablet):

1. dotare il dispositivo di una **password di accesso "robusta"**, avendo cura di mantenerla **riservata** (per la verifica sulla sicurezza della password, vedi http://www.passwordmeter.com/);
2. impostare il **blocco schermo** dopo un congruo tempo di inattività
3. dotare il dispositivo di sistemi **antivirus/antimalware aggiornati** ed effettuare una **scansione preventiva** all'inizio delle attività;
4. non lasciare dispositivi incustoditi ed accesi dopo aver compiuto l'accesso ai sistemi aziendali;
5. proteggere l'accesso alle **connessioni di rete** (ADSL, WIFI) con una password robuste;
6. evitare l'accesso a siti che non utilizzano **protocolli sicuri**, prestando che nella barra degli indirizzi compaia il formato; https://www.
7. qualora strettamente necessario, scaricare documenti unicamente da **siti affidabili**;
8. evitare l'uso di *social network* o altre applicazioni facilmente *hackerabili*;
9. predisporre una **postazione di lavoro dedicata** evitando che soggetti non autorizzati possano accedere, anche accidentalmente, alle informazioni ed ai dati personali trattati;
10. garantire il rispetto della riservatezza in occasioni di **conversazioni telefoniche**;
11. **evitare** di fare il ***download*** dei documenti di lavoro;
12. **stampare** documentazione contenente dati personali **solo quando necessario**, evitando di lasciare incustodite le copie prodotte e provvedere alla loro distruzione con modalità tali da rendere non conoscibili i dati ivi contenuti (es. sminuzzamento, triturazione);
13. utilizzare unicamente la **web-mail aziendale** per le comunicazioni di lavoro, evitando di utilizzare account di posta elettronica privati. **Evitare l'apertura di mail** provenienti da soggetti non affidabili, sia ricevute sull'indirizzo aziendale sia su quello privato;
14. non utilizzare dispositivi di archiviazione privati (USB, CD);
15. **NON salvare** documenti/files contenenti dati personali sul dispositivo privato.

Si chiede la massima collaborazione nell'approntare l'attività lavorativa al rispetto delle misure di sicurezza tecniche ed organizzative individuate, al fine di prevenire ogni possibile rischio per il sistema informatico aziendale e, in particolare, per i diritti e le libertà delle persone cui si riferiscono i dati personali.