PIANO INTEGRATO DI ATTIVITÀ E ORGANIZZAZIONE 2023-2025 - Allegato n. 6

ACCORDO INDIVIDUALE PER LA PRESTAZIONE LAVORATIVA IN MODALITA' LAVORO AGILE TRA

Il Direttore della U.O.C./ Dirigente U.O.S……,
afferente al Dipartimento/ Direzione ……
Dott./ Dott.ssa ……

E

Il/La dipendente assegnato/a alla Struttura sopra indicata
Sig./Sig.ra…… matricola n ……
nato/a……il……
residente a……, in via ……,
dipendente con rapporto di lavoro a tempo: indeterminato/ determinato e pieno/ parziale verticale (%.....) /parziale orizzontale (%.....)
con qualifica …… ….

CONSENSUALMENTE SI DEFINISCE QUANTO SEGUE

Dal giorno ……., per la durata di n. mesi ……, eventualmente rinnovabile, il dipendente lavorerà in modalità lavoro agile/lavoro da remoto nelle seguenti giornate settimanali:……
……
Il numero di giornate fruibili in modalità agile nel corso della settimana lavorativa è pari a ……;

Le giornate sopra indicate potranno essere modificate in funzione di eventuali necessità di servizio e dell'esigenza di assicurare un ottimale svolgimento delle attività lavorative. *(La modifica sarà comunicata dal responsabile di struttura al dipendente interessato e per conoscenza alla UOC Gestione del Personale,)* L'attività connessa allo svolgimento del lavoro agile sarà svolta dal dipendente presso il seguente indirizzo:
……
(indicare anche se trattasi di residenza, domicilio o altra sede).

Nell'arco della giornata lavorativa il dipendente deve essere reperibile e contattabile tramite e-mail e telefonicamente. Il recapito telefonico presso cui il dipendente è reperibile è il seguente:
……

Costituisce diritto del lavoratore la fruizione dei tempi di riposo e del conseguente diritto alla disconnessione, secondo quanto indicato nelle Liee guida, entro la durata della giornata lavorativa.

Il periodo temporale entro il quale il lavoratore non può erogare alcuna prestazione è individuato NELLA FASCIA ORARIA COMPRESA TRA …… E ……,
salvo esigenze eccezionali definite di comune accordo tra le parti.
Al lavoratore è fatto obbligo, inoltre, di rispettare i tempi di riposo di 15 minuti ogni 120 minuti di utilizzo del VDT.
L'attività è svolta mediante l'uso di PC aziendale e collegamento ADSL di proprietà del dipendente, salvo ipotesi eccezionali in cui potrà essere consentito l'utilizzo della propria strumentazione e ferme restante le misure di sicurezza.

In caso di utilizzo di programmi informatici aziendali il dipendente, qualora non fosse già stato abilitato in precedenza, dovrà, successivamente alla sottoscrizione del presente Accordo, da ambo le parti, richiedere alla UOC SIETC, l'attivazione della connessione remota sicura (VPN) e la messa a disposizione dei programmi necessari allo svolgimento della propria attività attraverso la apposita modulistica M.919.37-*MODULO DI RICHIESTA UTENZA APPLICATIVI* disponibile sulla intranet, nell'archivio documentale. Il modulo dovrà essere debitamente autorizzato dal direttore della struttura di appartenenza come previsto dal regolamento aziendale sulle risorse informatiche.

Le parti possono esercitare il diritto di recesso dal presente accordo individuale ai sensi dell'art. 19 della Legge 81/2017. In caso di accordo sia a tempo indeterminato che a tempo determinato, il recesso deve essere esercitato per iscritto, con preavviso non inferiore a trenta giorni. Nel caso di lavoratori disabili ai sensi dell'articolo 1 della legge 12 marzo 1999, n. 68, il termine di preavviso del recesso da parte del datore di lavoro non può essere inferiore a novanta giorni, al fine di consentire un'adeguata riorganizzazione dei percorsi di lavoro rispetto alle esigenze di vita e di cura del lavoratore.
In presenza di un giustificato motivo, ciascuno dei contraenti può recedere prima della scadenza del termine nel caso di accordo a tempo determinato, o senza preavviso nel caso di accordo a tempo indeterminato.

Costituisce giustificato motivo di recesso/sospensione:

A) **ragioni collegate al comportamento del lavoratore che**:
- non si sia reso reperibile nelle modalità e negli orari risultanti nel presente accordo per almeno 3 volte;
- In esito alle valutazioni periodiche compiute dal dirigente, risulti non aver svolto le attività indicate nel presente accordo
- In esito alle valutazioni periodiche compiute dal dirigente, risulti non aver conseguito gli obiettivi assegnati.

B) **ragioni di natura organizzativa che:**
- non consentano la prosecuzione dell'attività in regime di lavoro agile (a titolo meramente esemplificativo si fa riferimento ad ipotesi nelle quali le attività oggetto del presente accordo vengano assegnate ad UO diversa da quella di assegnazione del dipendente;

C) **ragioni di natura tecnica che:**
- non consentano la prosecuzione dell'attività in regime di lavoro agile;

D) **ragioni di natura personale:**
- gravi e documentati motivi personali del lavoratore

Il potere direttivo, espressamente richiamato nell'art. 2094 del c.c., si sostanzia nella possibilità per il datore di lavoro (dirigente) di impartire disposizioni segnatamente lo svolgimento dell'attività lavorativa. Tali disposizioni non possono essere disattese arbitrariamente dal lavoratore, eccetto i casi espressamente previsti dalla legge.
L'esercizio del potere direttivo nei confronti dei lavoratori che prestino servizio in regime di lavoro agile avviene, alla stregua di quanto si verifica per i lavoratori in presenza, mediante l'assegnazione di disposizioni e direttive da parte del Dirigente, in forma sia scritta che orale.

Il dipendente, con la sottoscrizione del presente Accordo, dichiara:
¬ di aver preso visione e di attenersi rigorosamente a quanto definito dalle linee guida;
¬ di aver preso visione ed attenersi scrupolosamente a quanto definito nei seguenti Allegati:

Allegato A "Norme di comportamento nell'utilizzo delle dotazioni informatiche per i dipendenti in lavoro agile",

Allegato B "Informativa sulla salute e sicurezza dei lavoratori in regime di smart working"

Allegato C "Addendum Privacy - Protezione dei dati personali lavoro agile" che, debitamente datati e firmati per accettazione, devono essere inviati, come parte integrante del presente accordo, alla UOC Politiche e Gestione del Personale.

¬ di manlevare l'Azienda da ogni responsabilità correlata all'utilizzo delle dotazioni informatiche, alla sicurezza e del rispetto della Privacy.

In caso di malattia o infortunio il dipendente deve tempestivamente avvisare il responsabile della struttura di assegnazione con le medesime modalità in vigore per le giornate di lavoro in sede. Durante le giornate di lavoro agile, le ordinarie funzioni gerarchiche naturalmente inerenti il rapporto di lavoro subordinato sono espletate per via telematica o telefonica.
Durante le giornate di lavoro agile il dipendente è tenuto a svolgere le seguenti attività:
……
……

Tali attività risultano funzionali al raggiungimento dei seguenti obiettivi:
……
……
……

Il raggiungimento degli obiettivi sarà verificato attraverso le seguenti modalità:
feedback permanente con il responsabile; report periodico; colloqui periodici con il dirigente;
……

La sottoscrizione del presente Accordo da parte del Direttore di Struttura equivale all'autorizzazione al lavoro agile nei confronti del dipendente richiedente.

Letto, confermato e sottoscritto.
Roma, lì _____

Il Dirigente della Struttura

Il Dipendente

Allegato A "Norme di comportamento nell'utilizzo delle dotazioni informatiche per i dipendenti in lavoro agile"

Durante l'attività di smart working (lavoro agile) il dipendente ha l'obbligo di rispettare tutti i regolamenti, le policy, le direttive, i codici di comportamento aziendali in vigore all'atto dello svolgimento dell'attività stessa, in particolare quanto indicato nel "Regolamento Aziendale Sull'utilizzo Delle Risorse Informatiche, Internet E Posta Elettronica" (REG/919/30) disponibile nell'archivio documentale sulla intranet aziendale.
Ogni strumento di lavoro (es. dispositivi, software, portali, …) messo a disposizione durante l'attività di smart working dall'Azienda, deve essere utilizzato con la massima cura, sia in termini di tenuta e conservazione (dispositivi), sia con rifermento alle modalità di accesso e al trattamento dati.
In particolare si ricorda che le credenziali di autenticazione alle postazioni e agli applicativi devono essere custodite con la massima diligenza e segretezza da parte dell'incaricato. È severamente vietato accedere alle postazioni di lavoro con credenziali altrui.
Rimangono valide ed efficaci per tutti i dipendenti in "smart working" le nomine a persona autorizzata al trattamento dei dati ai sensi del Regolamento 2016/679/EU e dell'art. 2 – quaterdecies del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, già conferite, così come le istruzioni con esse fornite nonché le misure di sicurezza attivate dall'Azienda e specificate nei regolamenti interni e nelle procedure aziendali.

Comportamenti specifici

Si rappresentano, di seguito, i principali comportamenti rientranti nell'ambito del presente regolamento che tutti gli utenti che effettuano l'attività lavorativa in smart working devono attuare al fine di tutelare se stessi e l'Azienda Ospedaliero Universitaria Sant'Andrea. In relazione alle diverse configurazioni possibili, caratterizzate dai diversi strumenti utilizzati, è necessario adottare comportamenti differenti, ma sempre coerenti con il principio di minimizzazione dei rischi correlati alla sicurezza informatica e con l'attuale normativa in ambito privacy.
L'unica configurazione possibile è attraverso l'accesso in VPN con MFA ai servizi/portali mediante la postazione di lavoro aziendale, usufruendo del proprio telefono personale per ottenere la password del FortiToken. Si ricorda che sul telefono personale non dovranno mai essere salvate le credenziali di dominio e di autenticazione.
Il "Manuale accesso in VPN MFA" è disponibile sulla intranet, nella sezione applicazioni aziendali (https://documentale.intraosa.net/storage/phocadownload/SistemiInformativi/Manuale%20utente%20AOUSA%20accesso%20VPN%20MFA_v1.0.pdf).
Si riportano di seguito le principali regole che devono necessariamente essere seguite dagli utenti.
Eventuali comportamenti difformi ricadranno direttamente sotto la responsabilità degli utenti stessi con tutte le eventuali conseguenze civili e penali correlate.

Giova ricordare in questa circostanza che un'eventuale compromissione della sicurezza informatica aziendale potrebbe comportare gravissime conseguenze sia in termini di continuità dei servizi erogati (amministrativi e sanitari) sia in termini di protezione dei dati aziendali, personali e/o sensibili trattati.

Utilizzo di servizi/portali con VPN e postazione di lavoro aziendale

Durante lo svolgimento dell'attività lavorativa in modalità smart working l'utente è autorizzato a memorizzare sul dispositivo aziendale eventuali file esclusivamente per il tempo strettamente necessario alla loro elaborazione; tale tempo non deve mai eccedere la sessione di lavoro quotidiana.

È vietata la detenzione sulle postazioni di lavoro di documentazione inerente all'attività lavorativa che violi il D.lgs. 101/2018 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.

Eventuali costi correlati alla connettività per l'acceso ad internet sono a carico del dipendente.

L'accesso al servizio di helpdesk è possibile utilizzando il pulsante "Invio segnalazioni" presente all'interno della Intranet aziendale o, in mancanza di accesso alla intranet, inviando una email al seguente indirizzo HRTI@ospedalesantandrea.it, altresì telefonando allo 0633775395.

L'utente è tenuto a conservare e custodire con la massima cura il dispositivo aziendale ricevuto e ad utilizzarlo esclusivamente per fini aziendali; qualsiasi malfunzionamento, danno da uso improprio o furto sono a carico dell'utente stesso.

Ulteriori misure di sicurezza da adottare durante lo svolgimento dell'attività lavorativa in modalità "smart working"

Durante tutte le operazioni di trattamento (raccolta, elaborazione, archiviazione, diffusione dei dati, ecc.), le informazioni messe a disposizione dall'Azienda devono essere conservate con la massima diligenza. Ogni documento, sia esso in formato elettronico che cartaceo, deve essere gestito garantendo un livello di sicurezza adeguato ad evitare il rischio di violazione dei dati (intendendosi per tale 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 rischio sussiste, infatti, sia nell'utilizzo di apparati di servizio informatici e telematici, sia nel caso di documenti cartacei.

Il dipendente deve garantire la riservatezza di tutte le informazioni di cui venga a conoscenza per il lavoro assegnatogli nonché di quelle derivanti dall'utilizzo delle apparecchiature, dei programmi e dei dati in essi contenuti.

L'utente deve adottare i seguenti comportamenti sia in relazione all'utilizzo di strumenti tecnici ed informatici di proprietà sia nel caso di utilizzo/accesso di strumenti messi a disposizione dall'Azienda, eventualmente anche mediante i primi, e segnatamente:

1. Collegarsi alla rete aziendale con le modalità sopra descritte, impedendo l'accesso ad altri soggetti non autorizzati (es. coniuge, parenti, amici).
2. In fase di avvio del PC devono sempre essere richieste le credenziali di accesso (no login automatico).
3. Le credenziali di accesso (username e password) devono essere conservate con diligenza, in modo che restino riservate, evitando che terzi non autorizzati possano conoscerle.
4. La password di accesso deve essere di lunghezza non inferiore a 12 caratteri; deve essere obbligatoriamente cambiata al primo utilizzo e successivamente almeno ogni 90 giorni; deve contenere, almeno 3 caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali (es. a@p23nZa2sa!); deve essere sempre diversa da almeno le ultime 10

precedentemente utilizzate; non deve presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti; deve essere nota esclusivamente all'utilizzatore e non può essere assegnata e/o comunicata ad altri; non deve contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti; non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere) o che si riferiscano ad informazioni personali; non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet.

5. Il computer ed eventuali altri strumenti in dotazione (smartphone, tablet, ecc.) non devono essere lasciati incustoditi e resi accessibili a persone non autorizzate. Nel caso del computer, l'utente è tenuto a disconnettere di volta in volta la sessione di lavoro, bloccando l'operatività del computer ed impedendo in tal modo indebiti accessi e/o visualizzazioni, anche solo accidentali, a persone non autorizzate.
6. Devono essere adottate tutte le misure necessarie ad evitare un utilizzo fraudolento o comunque non autorizzato della posta elettronica aziendale. L'accesso alla propria casella di posta elettronica al di fuori della rete aziendale deve avvenire con le seguenti modalità: utilizzando webmail va sempre evitato il salvataggio delle credenziali di accesso proposto dal browser, in ogni caso al termine della sessione di utilizzo procedere con la disconnessione effettuando il "logout".
7. La persona autorizzata non deve mai utilizzare dispositivi esterni di memorizzazione (esempio: chiavette usb, hard disk esterni, ecc.).
8. Salvaguardare adeguatamente lo strumento messo a disposizione dell'azienda per la connessione nonché i dati eventualmente in esso contenuti, evitando di lasciarlo incustodito presso e al di fuori del domicilio (es. nel transito dal domicilio alla sede del servizio) ed evitarne l'utilizzo per finalità personali, inserendo documenti e dati attinenti la propria sfera privata. Si ricorda, infatti, che tale pc è uno strumento di lavoro fornito dal datore di lavoro.

Il dipendente deve inoltre attenersi alle seguenti ulteriori istruzioni. Deve in particolare:

- Evitare che le conversazioni telefoniche di lavoro vengano ascoltate, anche involontariamente, da soggetti non autorizzati (es. coniuge, parenti, amici, conoscenti, estranei, ecc.);
- Evitare di detenere al domicilio documentazione cartacea contenente dati personali di cui l'Azienda è Titolare, a meno che ciò risulti indispensabile nell'ambito della gestione dell'emergenza epidemiologica e/o nello svolgimento delle proprie attività istituzionali e, in tal caso, garantirne una custodia adeguata ad impedire ogni possibile contatto, anche accidentale, tra i dati personali e persone non autorizzate, nonché adottare ogni misura di sicurezza utile a minimizzare i rischi di distruzione, perdita, modifica, divulgazione non autorizzata. Quando sia strettamente necessario trasportare da un luogo ad un altro (mediante mezzi pubblici o privati, o anche a piedi) documenti contenenti dati, gli stessi devono essere raccolti in porta documenti, riportanti l'identificazione del dipendente ed un suo recapito;
- Qualora sia necessario cestinare documenti cartacei, renderli per quanto possibile illeggibili strappando ad esempio più volte la carta, in modo che i contenuti diventino indecifrabili e non ricostruibili.

Si rende, infine, necessario adottare nello svolgimento dell'attività precise cautele, volte a prevenire, oltre che a limitare al massimo, il possibile rischio di violazioni di dati personali. In tale ottica, la persona autorizzata si impegna a segnalare tempestivamente qualunque evento relativo

a casi di violazione di dati personali (cd. data breach), al Titolare del trattamento per il tramite del proprio Delegato Privacy.
L'obbligo di segnalare senza indugio qualunque violazione di dati sussiste al fine di attivare le eventuali azioni conseguenti e necessarie, sulla base di quanto stabilito nella procedura aziendale di data breach e degli obblighi dal Regolamento (UE) 2016/679 e dal D.Lgs. 196/2003 come modificato dal D. Lgs.101/2018.

Accettazione del regolamento
Si ribadisce che il presente regolamento, comprese eventuali sue revisioni, è automaticamente considerato accettato dall'utente dal momento di inizio delle attività in modalità smart working (lavoro agile).

SISTEMA SANITARIO REGIONALE
AZIENDA OSPEDALIERO-UNIVERSITARIA
SANT'ANDREA

REGIONE LAZIO

SAPIENZA
UNIVERSITÀ DI ROMA

Allegato B "Informativa sulla salute e sicurezza dei lavoratori in regime di smart working"

Documento denominato "Manuale_Vol8_Smart_Working" presente sulla intranet aziendale al seguente link:

https://documentale.intraosa.net/storage/phocadownload/2021_5/Manuale_Vol8_Smart_Working.pdf , nella sezione EMERGENZA E SICUREZZA, sottosezione FORMAZIONE ED INFORMAZIONE dell'archivio documentale.

SISTEMA SANITARIO REGIONALE
AZIENDA OSPEDALIERO-UNIVERSITARIA SANT'ANDREA

REGIONE LAZIO
SAPIENZA UNIVERSITÀ DI ROMA

Allegato C "Addendum Privacy - Protezione dei dati personali lavoro agile"

In occasione della tua partecipazione alla modalità di erogazione della prestazione lavorativa denominata "Lavoro Agile" disciplinata dalla Legge n. 81/2017, ti ricordiamo 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 degli interessati che si relazionano con l'Azienda.

A tal fine si richiamano i contenuti delle informazioni fornite ex artt. 13 e 14 del Regolamento (UE) 2016/679 e norme di armonizzazione per il trattamento dei dati personali e categorie di dati personali dei dipendenti e degli utenti nonché dei regolamenti aziendali in materia, con le obbligazioni ivi riportate a carico dei singoli dipendenti in relazione al ruolo ricoperto nell'ambito dell'organigramma privacy aziendale e in ottemperanza al principio dell'accountability (responsabilizzazione).

Principi cardine:

- proteggi le informazioni riguardanti il tuo lavoro e la tua Azienda;
- non condividere con terzi dati, idee, soluzioni, opinioni che riguardano la tua attività lavorativa, potresti danneggiare il tuo lavoro e anche il tuo interlocutore;
- resta concentrato sull'attività lavorativa ovunque tu sia: sui documenti, sui file, sugli strumenti di lavoro; la distrazione può facilmente provocare smarrimenti, diffusione di informazione a soggetti non autorizzati, accessi non autorizzati, distruzione e perdita di dati, errori operativi che possono danneggiare i dati personali che si stanno trattando, gli interessati ai quali i dati si riferiscono; l'accuratezza nel fare le cose ti consente di lavorare in modo efficace ed efficiente anche al di fuori del contesto lavorativo;
- cura con scrupolosità le conversazioni, l'invio della mail, il salvataggio dei dati nel repository aziendale, il ricovero temporaneo di documenti in archivi estranei al perimetro aziendale abituale; la sistematica e schematica organizzazione delle risorse e degli strumenti di lavoro previene disguidi difficili da risolvere quando sei fuori dalla tradizionale sede di lavoro. Ogni file, ogni mezzo devono avere collocazioni e utilizzi abituali e sperimentati;
- mantieni la giusta separazione tra vita lavorativa e vita privata al fine di garantire la corretta esecuzione della prestazione lavorativa senza cagionarne e/o comprometterne la regolarità.

Il "Lavoro Agile" impone la massima attenzione sui temi della riservatezza e presuppone che il/la dipendente rimanga sempre concentrato sulle modalità di lavoro, al fine di svolgere la propria attività in modo corretto ed idoneo per proteggere l'operatività e la reputazione dell'Azienda. In particolare il "Lavoro Agile" non dovrà essere effettuato, a tal fine, al di fuori di ambienti privati

protetti, che garantiscano la necessaria riservatezza della prestazione e/o connettendosi con collegamenti WIFI a reti aperte.

Le conversazioni tra il/la 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/della 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;
- nel caso di conversazioni telefoniche instaurate a seguito di chiamate inoltrate o ricevute, accertare che l'interlocutore sia effettivamente un collega/cliente/fornitore legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione;

L'Azienda, in qualità di Titolare, stabilisce che, ai sensi dell'art. 24 comma 1 del Regolamento (UE) 2016/679, la documentazione inerente l'attività lavorativa dovrà risiedere esclusivamente nella cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al predetto Regolamento.

Il/La dipendente deve 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.

Per quanto riguarda la generica conservazione dei dati personali utilizzati dal/dalla dipendente in "Lavoro Agile" il Responsabile dell'unità organizzativa deve adottare soluzioni organizzative idonee a ridurre il più possibile i rischi di distruzione, perdita e accessi non consentiti ai dati anche in ambiente privato eletto dal/dalla dipendente.
Il "Lavoro Agile" non dovrà essere effettuato, a tal fine, al di fuori di ambienti privati protetti, che garantiscano la necessaria riservatezza della prestazione. Più in dettaglio, per quanto concerne l'utilizzo di documenti cartacei contenenti dati personali e prelevati dagli archivi dell'Azienda, si sottolinea che il trasferimento di dati personali all'esterno dell'Azienda deve essere giustificato da necessità strettamente correlate all'esercizio dell'attività lavorativa, agli obblighi di legge o alla difesa degli interessi dell'Azienda stessa.
La circolazione dei dati personali cartacei all'esterno dell'Azienda deve essere ridotta al minimo indispensabile; i dati devono essere raccolti in portadocumenti riportanti l'identificazione del/della dipendente utilizzatore e il suo recapito telefonico. In particolare i documenti cartacei:

- devono essere utilizzati unicamente per il tempo necessario allo svolgimento dei compiti assegnati e poi ripartiti negli archivi aziendali 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 fornite dal Regolamento Aziendale sull'utilizzo delle risorse informatiche,

internet e posta elettronica adottato con deliberazione n. 720/2021 che individuano, tra l'altro, le misure di sicurezza da adottare in caso di utilizzo di device personali e in particolare:

- la password di accesso deve essere conservata con diligenza in modo che resti riservata, evitando sotto la responsabilità del/della dipendente, che altri ne vengano a conoscenza;
- il computer ed altri eventuali strumenti in dotazione e/o utilizzati per l'espletamento delle prestazioni di "Lavoro Agile" (P.C., smartphone, personali e/o aziendali ecc.), non devono essere lasciati incustoditi ed accessibili a persone non autorizzate. In caso di allontanamento anche temporaneo dalla postazione di lavoro il/la 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.

I trattamenti effettuati dal/dalla dipendente devono rispettare il principio di necessità, pertinenza e non eccedenza rispetto alle finalità degli stessi, avere scopi espliciti, determinati e leciti, come da istruzioni fornite in punto all'atto dell'autorizzazione al trattamento dati dell'Ente.

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' fondamentale sottolineare che è severamente sanzionata dal Regolamento (UE) 2016/679 la violazione dei dati personali, 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"(comprese le ipotesi di sottrazione e/o furto), 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 l'Azienda la Notifica del Data Breach, cioè la comunicazione della violazione dei dati personali all'Autorità di Controllo (Garante per la protezione dei dati personali), nonché, qualora ne abbiano un danno, ai soggetti i cui dati sono stati violati.
A tal fine si ribadisce l'obbligo del/della dipendente di segnalare qualunque ipotesi di violazione dei dati personali al responsabile della struttura preposto e al Responsabile della Protezione dei Dati, tempestivamente e, comunque, nei termini previsti dalla Procedura interna di Data Breach, anche al fine di consentire il rispetto dei ristretti termini di notifica all'Autorità di Controllo previsti dal Regolamento (UE) 2016/679, ove atto dovuto.
Rimangono valide ed efficaci per tutti i dipendenti in "Lavoro Agile" le nomine a persona autorizzata al trattamento dei dati ai sensi del Regolamento 2016/679/EU e dell'art. 2 – quaterdecies del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, già conferite, così come le istruzioni con esse fornite nonché le misure di sicurezza attivate dall'Azienda e specificate nei regolamenti interni e nelle procedure aziendali. Pertanto il presente addendum integra le predette nomine già conferite e le istruzioni ivi contenute.
E' obbligazione contrattuale del/della dipendente rispettare dette istruzioni e partecipare alle attività formative in materia previste dell'Azienda.
Il/La dipendente è consapevole ed accetta che AOUSA verifichi il rispetto delle misure di sicurezza informatiche ed operative che Gli/Le sono state indicate all'atto dell'autorizzazione alla modalità operativa del "Lavoro Agile", nel rispetto delle previsioni della normativa vigente in materia e dell'art.4 della L.300/70 e s.m.i..

Per ricevuta e accettazione

Data _____ Il Dipendente _____