Il Dipendente (indicare Cognome e nome leggibile)

_____

**Oggetto: Integrazione all'Atto di designazione ai sensi dell'art. 2-quaterdecies del D.Lgs. n. 196/2003 e s.m.i. e dell'art. 29 del Regolamento UE 2016/679 in seguito, "GDPR")**

**Premesso che:**

- ASST della Valtellina e dell'Alto Lario è Titolare del trattamento dei dati personali ai sensi dell'art. 4, n. 7 del Regolamento Generale sulla Protezione dei dati personali UE 2016/679 (di seguito "Regolamento" o "GDPR") e del D.Lgs n. 196/2003, come modificato dal D.Lgs n. 101/2018 (di seguito "Codice privacy"), con le responsabilità che discendono dalla citata normativa e dalle ulteriori norme, provvedimenti e linee guida integrative adottate dal legislatore nazionale, dall'Autorità Garante per la protezione dei dati personali e dall'European Data Protection Board (di seguito, unitariamente definiti anche come "Norme e Provvedimenti vigenti");
- ai sensi dell'art. 2-quaterdecies del D.Lgs n. 196/2003, come modificato dal D.Lgs n. 101/2018, il Titolare del trattamento può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, «*che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche espressamente designate*» che operano sotto la sua autorità e può individuare, a tal scopo, le modalità più opportune per autorizzarne il trattamento;
- secondo quanto disposto dall'art. 29 del GDPR, chiunque agisca sotto l'autorità del Titolare ed abbia accesso ai dati personali può trattare tali dati esclusivamente se è istruito dal Titolare del trattamento2-.stata formalmente autorizzata al trattamento dei dati personali trattati al fine di espletare le mansioni connesse al ruolo di _____ che le è stato affidato in quanto dipendente dell'ASST;
- a causa dell'emergenza Coronavirus, le vigenti disposizioni normative nazionali e regionali individuano il cd. smart working quale una delle modalità ordinarie di svolgimento dell'attività lavorativa.

**Tutto ciò premesso e considerato,**

ad integrazione di quanto già disposto con apposito l'Atto di designazione da lei sottoscritto e con precipuo riferimento alle attività che lei svolgerà presso il suo domicilio in attività di smart working, il Titolare ai sensi dell'art. 2-quaterdecies del D.Lgs n. 196/2003 e s.m.i. e dell'art. 29 del Regolamento UE 2016/679, fornisce le seguenti specifiche indicazioni ed istruzioni.

L'attività lavorativa, laddove non potrà essere svolta tramite strumenti aziendali, potrà essere svolta tramite strumenti personali.

Nell'espletamento delle attività lavorative in modalità Smart Working lei è tenuta/o ad osservare scrupolosamente quanto disposto dalle "**Linee guida per il trattamento dei dati personali nelle attività di smart working**" adottate dall'ASST ed allegate, per sua conoscenza, alla presente.

Ciò posto, si ricorda che i dati personali comunque raccolti dovranno essere trattati in modo lecito, corretto e non eccedente rispetto alle finalità per le quali sono stati raccolti. Gli stessi dovranno altresì essere registrati ed utilizzati esclusivamente per scopi attinenti alle mansioni assegnate.

Nessun dato potrà essere comunicato e/o diffuso a soggetti non autorizzati in qualunque forma per finalità diverse da quelle sopra elencate, se non previa autorizzazione del Titolare del trattamento dei dati.

Lei dovrà operare nel rispetto di Norme e Provvedimenti vigenti, in conformità al Modello di Governance della Privacy della ASST della Valtellina e dell'Alto Lario, nonché secondo le eventuali ulteriori istruzioni sui trattamenti impartite dal Titolare e dal DPO.

Lei dovrà operare prestando la massima collaborazione, consultandosi eventualmente anche con il DPO, nonché avvalendosi delle figure specificamente competenti in tema di privacy individuate all'interno della Sua Funzione.

Lei è poi tenuta/o a cooperare e rispondere tempestivamente e in modo esaustivo in relazione a ogni richiesta, anche informativa, da parte del Titolare e del DPO.

Gli effetti della presente Lettera d'incarico cesseranno al cessare dello stato di emergenza

in essere previa formale comunicazione del Titolare, salva la facoltà di revoca in qualunque momento da parte del Titolare.

In ogni caso, lei presterà la piena cooperazione a tutte le attività conseguenti alla cessazione.

Eventuali violazioni della presente nomina, degli obblighi normativi o contrattuali, nonché delle disposizioni regolamentari interne in materia di protezione dei dati personali costituiscono inadempimento degli obblighi contrattuali, con applicazione delle sanzioni disciplinari previste dal vigente contratto di lavoro.

**All. 1 "Linee guida per il trattamento dei dati personali nelle attività di smart working"**

Sondrio, lì _____

**Il Titolare del trattamento**

**ASST della Valtellina e dell'Alto Lario**

_____

**per presa visione ed integrale**

**accettazione dei compiti e delle funzioni attribuite**

**All. 1**

# LINEE GUIDA PER IL TRATTAMENTO DEI DATI PERSONALI NELLE ATTIVITÀ DI SMART WORKING

## CONTESTO

Ai fini delle presenti Linee Guida si intende per lavoro agile, o "smart working", una peculiare modalità di esecuzione dell'attività lavorativa che può esser resa all'esterno della sede di lavoro, senza una postazione fissa.

L'introduzione del lavoro agile all'interno dell'ASST della Valtellina e dell'Alto Lario risponde anche alle esigenze di contenimento e gestione dell'emergenza del virus COVID-19 (Coronavirus), espressamente rilevate dai provvedimenti normativi adottati nell'ambito della fase emergenziale in essere.

## SCOPO

Premesso che il personale individuato dovrà svolgere la propria attività lavorativa all'esterno delle sedi e strutture aziendali, avvalendosi di strumentazione aziendale e personale, nel rispetto della normativa di tutela della privacy e di sicurezza dei dati personali trattati, le presenti Linee Guida hanno l'obiettivo di fornire indicazioni circa le modalità di svolgimento dell'attività lavorativa e le cautele da adottare al fine di ottemperare alle disposizioni di cui al D.Lgs. 196/2003 ed al Regolamento UE/679/2016.

## INDICAZIONI OPERATIVE

La prestazione lavorativa resa con la modalità smart working è integralmente considerata come servizio pari a quello ordinariamente reso presso le sedi abituali di lavoro, pertanto anche nell'espletamento di tale attività il lavoratore è tenuto a custodire ed utilizzare con diligenza la documentazione, i dati e le informazioni utilizzati per l'esecuzione della prestazione.
Si precisa altresì che il lavoratore è tenuto al rispetto delle previsioni del Regolamento UE 679/2016 e del D.Lgs. 196/2003 in materia di protezione dei dati personali e che l'inosservanza delle predette disposizioni costituisce un comportamento rilevante ai fini disciplinari e può conseguentemente determinare l'applicazione delle sanzioni disciplinari previste dalla contrattazione collettiva applicata.

1. <u>STRUMENTAZIONE E SEDE</u>

È consentito il lavoro agile ai possessori di PC portatili/fissi, che abbiano una connessione internet propria (es. ADSL, Hotspot da Smartphone).
Se si utilizza lo strumento aziendale, il SIA provvede alla configurazione (installazione della VPN) in modo che da casa al lavoratore sia possibile l'accesso alle reti aziendali necessarie allo svolgimento dell'attività lavorativa.

Nei casi in cui non sia possibile per l'azienda attivare la VPN, il lavoratore è autorizzato - in deroga alle istruzioni conferite al momento di assunzione dell'Incarico come previsto dalle norme emergenziali – a copiare su dispositivi rimovibili e/o inviare tramite email il materiale necessario per l'espletamento dell'attività lavorativa.

Per l'espletamento dell'attività lavorativa, il dipendente è altresì autorizzato a portare presso il proprio domicilio la documentazione cartacea limitatamente a quella rilevante e necessaria per l'espletamento delle proprie attività, anche quando contenente dati personali.

Tutti gli strumenti di lavoro impiegati, cartacei ed elettronici, dovranno in ogni caso essere obbligatoriamente conservati con modalità idonee a garantirne la sicurezza e l'integrità.
Pertanto, il dipendente è tenuto a scegliere sedi di lavoro e di archiviazione/custodia del materiale che siano idonee secondo criteri di sicurezza, integrità fisica e massima riservatezza delle informazioni e dei dati trattati nell'espletamento delle proprie mansioni.
Il lavoratore dovrà ad esempio prediligere postazioni di lavoro collocate in parti dell'immobile riservate, ovvero il cui accesso può essere inibito ad altri componenti del nucleo familiare.
Parimenti, il dipendente è tenuto a non svolgere l'attività lavorativa in *outdoor*, quando tale modalità può rendere le informazioni trattate accessibili a soggetti terzi non autorizzati (i.e. confinanti, abitanti di immobili prossimi, ecc.).

## 2. CONFIGURAZIONE DEI DISPOSITIVI

Nei casi in cui l'espletamento delle attività lavorative comporti l'utilizzo di dispostivi elettronici e/o telefonici, il dipendente dovrà attenersi alle seguenti indicazioni:

### 2.1. Dispositivi aziendali

Il dipendente è tenuto a non modificare le impostazioni di sicurezza presenti sul dispositivo assegnato e ad utilizzare lo stesso secondo le modalità ordinarie.
Il dipendente è altresì tenuto ad utilizzare il dispositivo esclusivamente per le attività lavorative, essendo assolutamente vietato accedere a social network o a qualsiasi sito web o server mail che non appartenga a quelli già preventivamente impostati.

### 2.2. Dispositivi personali

Il dipendente è tenuto ad utilizzare i dispositivi solo ove gli stessi presentino adeguate caratteristiche di sicurezza e protezione delle informazioni trattate.
Si richiede ad esempio che il pc o altro dispositivo utilizzato abbia:

- un sistema antivirus aggiornato,
- un account, dedicato all'attività lavorativa se usato anche da familiari o conviventi, protetto con password,
- modalità automatica di inserimento del blocco pc in caso di inattività prolungata.

Per i dispositivi di tipo telefonico, il dipendente è tenuto ad utilizzare lo strumento personale solo quando strettamente necessario ed in ogni caso è tenuto a cancellare immediatamente a seguito dell'utilizzo i dati sullo stesso eventualmente transitati.

Indipendentemente dalla natura aziendale o personale del dispositivo, ogni dipendente è tenuto a non lasciare il dispositivo incustodito o accessibile a terzi e non allontanarsi dalla postazione di lavoro, anche in ambiente domestico, senza che ogni dato trattato sia adeguatamente protetto.
Si ricorda altresì di limitare il salvataggio in locale dei dati ai casi eccezionali, ovvero alle sole ipotesi in cui non sia possibile tecnicamente lavorare direttamente sulla rete aziendale mediante accesso tramite VPN, e di eliminare i suddetti dati tempestivamente una volta cessata l'esigenza.

3. GESTIONE DI CREDENZIALI E PASSWORD

L'accesso ai dispositivi, personali ed aziendali, nonché ai software forniti dall'Azienda anche in tale fase emergenziale è soggetto obbligatoriamente ad autenticazione.
Lo stesso avviene pertanto attraverso un sistema di autenticazione e autorizzazione basato su credenziali di accesso, consistenti in un codice per l'identificazione dell'utente ("username" o "nome utente") ed una parola chiave riservata ("password").

Tutti i dipendenti sono tenuti a rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso di seguito indicati:

- non utilizzare combinazioni facili da identificare (creare password con lunghezza non inferiore ad 8 caratteri, con almeno 2 caratteri tra numeri e caratteri speciali (es. @), non coincidente con la precedente password per almeno tre caratteri, non contenente riferimenti agevolmente riconducibili all'utente);
- non comunicare/condividere le credenziali con altri soggetti, neppure se appartenenti all'Azienda,
- prestare attenzione a rispondere ad e - mail sospette e/o a cliccare sui link durante la navigazione web (o nella mail) al fine di contrastare possibili frodi informatiche (come il phishing, lo spear phishing, il furto d'identità, ecc.).

Si ricorda che ogni utente è responsabile di tutte le azioni e le funzioni svolte dal suo account. Qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi o abbiano in altro modo perso la propria natura riservata, l'utente dovrà tempestivamente avvisare il SIA ed immediatamente procedere alla loro modifica.

Si ricorda che è vietato salvare sul desktop del dispositivo personale le credenziali di accesso agli applicativi aziendali.

4. GESTIONE DI DATA BREACH

Si ricorda che l'art. 33 GDPR prevede che il Titolare del Trattamento deve notificare all'Autorità Garante e comunicare agli interessati un evento di "*personal data breach*", intendendosi per "*data breach*" l'accesso non autorizzato ai dati personali, la distruzione accidentale o la perdita dei dati, la divulgazione, modificazione, copia o rimozione dei dati in assenza di autorizzazione.

Affinché l'ASST possa adempiere all'obbligo di notifica all'Autorità ex art. 33 GDPR, il soggetto incaricato al trattamento, ogni dipendente, è tenuto a segnalare immediatamente un sospetto di violazione o una violazione accertata attraverso l'invio di email all'Ufficio Privacy e al DPO, nonché laddove siano coinvolti gli Strumenti Aziendali al SIA.
Nei casi di urgenza e di impossibilità di procedere all'invio di comunicazione email, il dipendente è tenuto a contattare telefonicamente il proprio Responsabile e ad inviare un'email ai soggetti sopra indicati non appena possibile.

Contatti:
Ufficio Privacy <ufficio.privacy@asst-val.it>
Dpo <dpo@asst-val.it>

Si precisa che la mancata notifica di un *data breach* comporta l'applicazione di sanzioni amministrative pari all'importo maggiore tra € 10.000.000 e il 2% del fatturato complessivo dell'esercizio precedente e che in caso di violazione anche di altre disposizioni del GDPR le sanzioni possono arrivare all'importo maggiore tra € 20.000.000 e il 4% del fatturato complessivo dell'esercizio precedente. Resta poi salva la responsabilità risarcitoria nei confronti dell'interessato, il quale ha diritto al risarcimento dei danni materiali o immateriali causati dalla violazione del GDPR da parte del Titolare del trattamento.

## 5. REGOLE GENERALI

In via generale, si ricorda che ogni dipendente è tenuto a:

- seguire prioritariamente le policy e le raccomandazioni fornite dall'ASST,
- assicurarsi che i software di protezione del sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati,
- non installare software provenienti da fonti/repository non ufficiali,
- non cliccare su link o allegati contenuti in email sospette,
- collegarsi a dispositivi mobili (pen-drive, hdd-esterno, ecc.) solo se ne è nota la provenienza o se forniti dall'ASST,
- evitare di comunicare con i colleghi tramite mezzi diversi da quelli indicati dall'ASST,
- effettuare sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa,
- evitare di condividere con i colleghi documenti aziendali o attività lavorative su piattaforme diverse da quella aziendale o da quella indicata dal SIA,
- evitare di condividere con i colleghi le proprie credenziali di accesso,
- evitare di postare sui social o inviare a terzi foto atte a documentare l'attività di smart working stante il rischio di esporre a pericolo di diffusione illegittima dati personali eventualmente presenti sul monitor.