



## REGOLAMENTO UE 2016/679 INFORMATIVA SMARTWORKER

Gentile Dipendente

Vista la condizione emergenziale, dovuta al propagarsi del Coronavirus, il Governo, d'urgenza, ha stabilito con il **DPCM 23.02.2020** e il **DPCM 4.03.2020** ribadito con l'**Accordo del 14 marzo 2020** - anche in assenza dell'accordo individuale - l'attivazione immediata su tutto il territorio nazionale dello *Smart Working* o *Lavoro Agile* (art. 18 L. 81/2017), per tutti i tipi di lavori per cui risulti attuabile.

L'azienda, attenendosi alle disposizioni governative, la invita a prendere atto del presente incarico, al fine di espletare le Sue prestazioni in linea con la disciplina del Reg. 2016/679 (GDPR) e del D. Lgs. 101/18, rispettando le seguenti disposizioni:

### REGOLAMENTO PRIVACY PER LO SMART WORKING / LAVORO AGILE

Le prestazioni contrattuali svolte, che possono comportare il trattamento di dati personali, sono già state oggetto di specifico incarico o autorizzazione privacy ai sensi degli artt. 4, 29, 32 e 39 del Reg. 2016/679, con apposita lettera di incarico, il cui contenuto si intende integralmente richiamato e costituisce parte integrante della presente e è da considerare applicabile anche nell'attuale condizione di Smart Worker. In particolare, oltre ai doveri previsti dalle norme di legge, si segnalano i seguenti doveri:

- non violare il segreto e la riservatezza delle informazioni trattate;
- proteggere i dati contro i rischi di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito;
- rispettare e applicare le misure di sicurezza fisiche, informatiche, organizzative, logistiche e procedurali;
- rispettare e applicare il Regolamento per l'utilizzo degli strumenti informatici ed elettronici, per l'utilizzo della posta elettronica, di internet e delle App.

Si avverte che prima di compiere qualsiasi attività difforme da quanto sopra richiamato occorre assolutamente rivolgersi al proprio referente gerarchico superiore o al titolare del trattamento o all'amministratore di sistema per ottenere eventuale autorizzazione. Agli stessi soggetti occorre immediatamente comunicare qualsiasi anomalia informativa riscontrata nel sistema oppure verificatasi durante l'attività (il Tablet è caduto ma sembra funzionante, lo screen saver non appare più, ecc...).

Si avverte altresì che nella attuale condizione di Smart Worker si impongono, per ragioni di riservatezza, le seguenti condizioni:

- individuare in casa una stanza o comunque uno spazio deputato per allestire la postazione lavorativa, che possa essere utilizzato in modo esclusivo, interdicendone l'accesso agli altri





familiari, con possibilità di chiusura della porta a chiave, con armadietti dotati di serratura ove riporre la documentazione e/o gli strumenti di lavoro;

- assicurarsi della conformità delle prese elettriche domestiche prima di utilizzarle per alimentare il dispositivo o i dispositivi aziendali;
- assicurarsi che la postazione scelta non possa essere investita da acqua, fuoco, vento, calore eccessivo;
- evitare di lasciare incustodita la postazione e, al termine di ogni sessione lavorativa, riporre tutto negli armadietti chiusi a chiave;
- utilizzare il dispositivo mobile aziendale solo ed esclusivamente per le attività lavorative, evitando assolutamente di utilizzarlo per accedere a social network o a qualsiasi sito web o server mail, che non appartenga a quelli già preventivamente impostati dall'amministratore di sistema;
- evitare di inserire nel dispositivo aziendale pennette USB o comunque basi dati esterne ed evitare di scaricare applicazioni non autorizzate dall'azienda;
- evitare assolutamente di salvare le password sul browser ove non siano ancora state attuate le credenziali di accesso multifattore;
- evitare di comunicare con i colleghi tramite mezzi diversi da quelli indicati dal datore di lavoro;
- evitare di postare ai colleghi le proprie credenziali di accesso;
- evitare di condividere con i colleghi documenti aziendali o attività lavorative su piattaforme come Google document ovvero altre simili e/o comunque piattaforme diverse da quella aziendale o da quella indicata dal datore di lavoro;
- evitare di attingere la connettività dal modem o dalla Wi-Fi di casa o da hot spot sconosciuti oppure da hot spot pubblici o comunque da qualsiasi altra fonte che non sia quella indicata o già impostata dall'azienda;
- comunicare al datore in modo preciso e puntuale gli orari di lavoro che comunque devono assolutamente essere individuati in fasce giornaliere corrispondenti a quelle in cui si svolge o si svolgeva l'attività aziendale al fine di avere un immediato supporto in caso di anomalie informative e/o informatiche;
- spedire al termine di ogni giornata lavorativa un breve report al datore di lavoro in merito alle informazioni trattate, a eventuali condivisioni di documenti con i colleghi o ai colloqui con essi, alle conferenze via Skype o simili intercorse con fornitori, clienti, partner o qualsiasi altro soggetto, al fine di poter risalire la catena delle attività compiute in caso di esigenze di recupero dati e/o informazioni;





- comunicare immediatamente al datore di lavoro qualsiasi situazione di potenziale o effettivo attacco Hacker o altra condizione che possa compromettere la sicurezza dei dati trattati;
- di non disattivare e mantenere attive le protezioni sul dispositivo utilizzato per fini aziendali, come le altre misure di sicurezza trattati nell'incarico generale.

Tutto quanto sopra esposto costituisce attualmente - sebbene suscettibile di modifiche e/o integrazioni - il Regolamento Data Protection che lo Smart Worker è tenuto ad osservare. Tutti gli obblighi sopradescritti fanno parte integrante della prestazione lavorativa e a cui ogni lavoratore è tenuto in base al contratto di lavoro.

La presente autorizzazione/istruzione ha efficacia fino a quando non verrà revocata la modalità Smart Working da parte del datore di lavoro.

Arezzo, 30.03.2020

**Il Titolare del Trattamento**

