

## ACCORDO AZIENDALE

### INSTALLAZIONE ED IMPLEMENTAZIONE DEL SOFTWARE ZSCALER

Tra

- la Società UCI ITALIA SPA con sede legale in Cernusco Sul Naviglio, Via Carlo Donat Cattin, 5, Capitale Sociale Euro 1.120.000,00 i.v., codice fiscale e numero di iscrizione Registro Imprese di Roma 04342801000, in persona della Dott.ssa Eva Maria Valles quale Direttore del dipartimento People SE e della Dott.ssa Filomena Zaccaro quale People Business Partner per l'Italia,
- la SLC-CGIL nazionale nella persona di Umberto Carretti
- la FISTel-CISL nazionale nella persona di Sabria Sharif
- la Uilcom- UIL nazionale nella persona di Roberto Corirossi
- L'Anec associazione datoriale nella persona di Arnaldo Ciulla  
in rappresentanza dei lavoratori

#### PREMESSO CHE

- a) UCI ITALIA esercita l'attività di gestione e programmazione di sale cinematografiche ed in tale ambito gestisce diverse sedi sul territorio italiano nel quale sono occupati lavoratori dipendenti;
- b) Ogni lavoratore ha a disposizione, come strumento di lavoro concesso in dotazione dall'azienda, computer portatili o fissi individuali o in condivisione sui cinema ai fini dello svolgimento dell'attività lavorativa
- c) Al fine di gestire e monitorare la sicurezza dei dati aziendali, l'azienda ha applicato e utilizzato sistemi di proxy a livello locale, diversi per ogni paese della regione del Sud Europa;
- d) Da un'analisi approfondita e, a seguito di alcuni attacchi alla sicurezza dei dati aziendali in UK e in Spagna, in diverse occasioni, è stato riscontrato che gli strumenti in uso non sono sufficientemente sicuri e protettivi del business;
- e) Da queste premesse è nato un progetto e una visione strategica della gestione dei dati aziendali condivisa da tutto il gruppo Odeon Cinemas Group, includendo anche la regione del Sed Europa di cui l'Italia è parte;

*d* *Sh*

- f) Tra i vari software oggi disponibili sul mercato informatico, le migliori prestazioni in termini di sicurezza, allineate alle necessità del nostro business, sono state individuate nel software ZScaler;
- g) Il sistema impedirà a tutti i dispositivi di OCG di accedere e/o contattare servizi ritenuti dannosi per l'azienda, garantendo quindi accesso sicuro ai dipendenti e alle informazioni aziendali;
- h) l'implementazione di questo sistema rispecchia la volontà aziendale di avere un valido strumento di tutela del business aziendale, applicato in maniera omogenea a tutto il circuito OCG, applicabile e utilizzabile come monitoraggio sia nella fase di lavoro svolto in ufficio, sia nei casi di lavoro da remoto (per il personale di sede)

Dato atto che le premesse sono parte integrante e sostanziale del presente accordo, le Parti convengono quanto segue:

### **1. Installazione ed uso del sistema Zscaler**

L'installazione del sistema avrà come unica finalità la tutela della sicurezza del business aziendale.

L'Applicazione raccoglie e registra informazioni su tutti i siti che il dipendente ha visitato o ha tentato di visitare, nonché l'indirizzo IP da cui provengono ma le informazioni vengono utilizzate per mantenere la sicurezza delle informazioni tecniche del gruppo, vale a dire per individuare tentativi di attacco e per indagare su problemi di sicurezza informatica (compresi eventuali eventi di perdita di dati).

I dati rilevati e registrati non verranno utilizzati per finalità diverse da quelle imposte dalla necessità di sicurezza. Tale applicazione non è finalizzata al controllo a distanza diretto, indiretto o anche accidentale dell'attività e del comportamento dei dipendenti.

I dati salvati non potranno essere utilizzati per fini strettamente valutativi;

L'informativa allegata al presente accordo, che sarà condivisa con tutti i dipendenti, chiarisce nel dettaglio le modalità di installazione e gestione del sistema in azienda.

Chiarisce che il sistema terrà traccia delle azioni del dipendente sugli accessi ad internet ma non dei contenuti consultati o inseriti sulla pagina di interesse.

### **2. Gestione del sistema Zscaler**

E' in carico al dipartimento IT.



In particolare la cura dei report delle attività dei dipendenti verranno custodite e rese visibili ad un solo unico Group Platform Team Specialist per tutto il Gruppo OCG.

Eventuali necessità di accesso ai report delle attività, custodite per soli 12 mesi, potranno avvenire solo dietro un triplo livello di approvazione dalle seguenti posizioni in azienda:

- Managing Director della Regione del Sud e del Nord Europa
- Group Chief People Officer, referente risorse umane di tutta OCG
- People Director della Regione del Sud Europa

L'accesso ai report avverrà solo per specifiche situazioni di rischio aziendale che, in via ipotetica e pre-applicazione del sistema, possiamo prevedere in rischi di attacco informatico o problematiche tecniche di natura informatica; rischi o segnalazioni legate a questioni legali; rischio di frode per l'azienda. Si definisce che queste tipologie di motivazioni sono puramente indicative e non pienamente esaustive.

### 3. Controlli e verifiche della corretta applicazione

Il Data Protection Officer, esterno all'azienda, sta valutando l'applicazione di verifiche e controlli al fine di tutelare e garantire la massima protezione dei dati in linea e in accordo con le privacy policy del gruppo OCG e al regolamento UE 679/2016.

### 5. Validità dell'accordo

Le parti s'impegnano con la firma del presente accordo, fermo restando l'impegno a garantire l'applicazione del sistema al solo fine di sicurezza aziendale e non di monitoraggio o controllo del dipendente.

Il presente accordo potrà essere oggetto di nuove discussioni qualora il sistema modificasse la natura e/o la funzione di cui sopra rappresentato.

Letto, confermato e sottoscritto il giorno 19 ottobre 2022

PER L'AZIENDA 

PER ANEC 

PER LE OO.SS.

SLC-CGIL 

FISTel-CISL *Sabria Sharif*

Uilcom- UIL 