

## Verbale di accordo

Il giorno 16 aprile 2019 presso la sede Italiaonline di Assago si sono incontrate

**ITALIAONLINE S.P.A.** (di seguito la "Società" o l'"Azienda"), con Consodata S.p.A.

e le **Segreterie nazionali delle Organizzazioni sindacali SLC-CGIL, FISTel-CISL e UILCOM-UIL,**

unitamente ad una rappresentanza di RSU

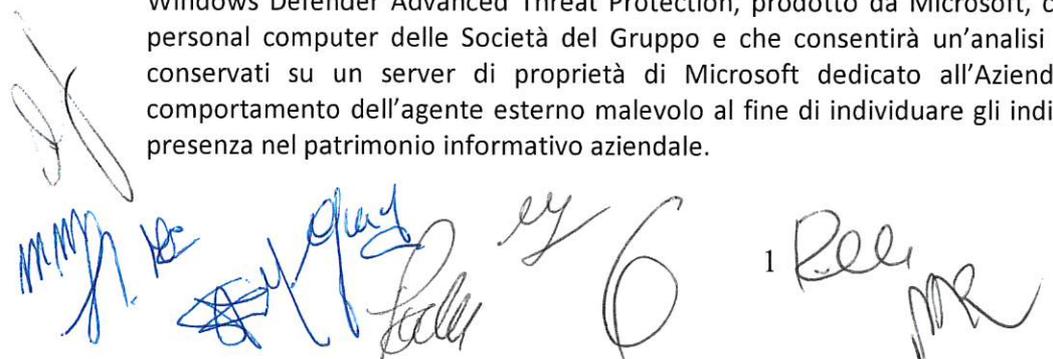
(di seguito congiuntamente anche "le Parti")

### **Premesso che:**

- l'art. 4, comma 1 della Legge 300/1970, così come modificato dall'art. 23 del D.lgs. 151/2015 e s.m.i. stabilisce che "gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali";
- in un contesto tecnologico profondamente evoluto e dinamico, le soluzioni di sicurezza attualmente presenti in Azienda non risultano più adeguate a garantire la sicurezza delle informazioni in quanto non più in grado di rilevare e contrastare le nuove tipologie di minacce e di attacchi informatici, sempre più invasivi e sofisticati;
- al fine di proteggere l'Azienda, i clienti e i dipendenti ed i loro dati da attacchi cyber come ad esempio quelli realizzati inducendo ad attivare link ricevuti per email, aprire allegati o rispondere fornendo inconsapevolmente dati personali o aziendali, l'Azienda ritiene necessario introdurre nuovi strumenti che siano adeguati allo stato dell'arte, assieme a nuovi processi che contemplino l'adozione delle più recenti metodologie di sicurezza necessarie per far fronte ad un cambiamento sempre più rapido degli scenari di attacco cyber;
- nel corso dell'incontro odierno sono state ampiamente ed esaurientemente presentate le ragioni che hanno indotto l'Azienda a introdurre metodologie di sicurezza per fronteggiare attacchi cyber, nonché le caratteristiche e le funzionalità dello strumento che verrà utilizzato all'uopo.

### **Le Parti convengono quanto segue:**

successivamente alla sottoscrizione della presente intesa, verrà introdotto in azienda lo strumento Windows Defender Advanced Threat Protection, prodotto da Microsoft, che verrà installato su tutti i personal computer delle Società del Gruppo e che consentirà un'analisi da remoto (i dati verranno conservati su un server di proprietà di Microsoft dedicato all'Azienda) basata sullo studio del comportamento dell'agente esterno malevolo al fine di individuare gli indicatori che ne identificano la presenza nel patrimonio informativo aziendale.

The bottom of the page features several handwritten signatures in blue ink. From left to right, there is a large, stylized signature, followed by a smaller one, then a signature that appears to be 'Gual', another signature, a signature that looks like 'ey', a large circular mark, and finally a signature that starts with '1 Reel'.

La successiva ricerca dello specifico indicatore individuato mediante l'analisi comportamentale sull'intero insieme dei dati dell'azienda potrà portare ad identificare la presenza di una minaccia in tempo utile per limitarne l'impatto, sia in termini di perdita di dati personali e di business, che di funzionalità e produttività dei sistemi informatici aziendali.

Lo strumento informatico descritto verrà introdotto al solo scopo di tutelare il patrimonio e il sistema informativo aziendale. Di conseguenza l'utilizzo di nuovi strumenti e processi di sicurezza informatica non è finalizzato al monitoraggio del comportamento del dipendente per valutarne prestazioni e/o rendimento professionale e conseguenti contestazioni disciplinari.

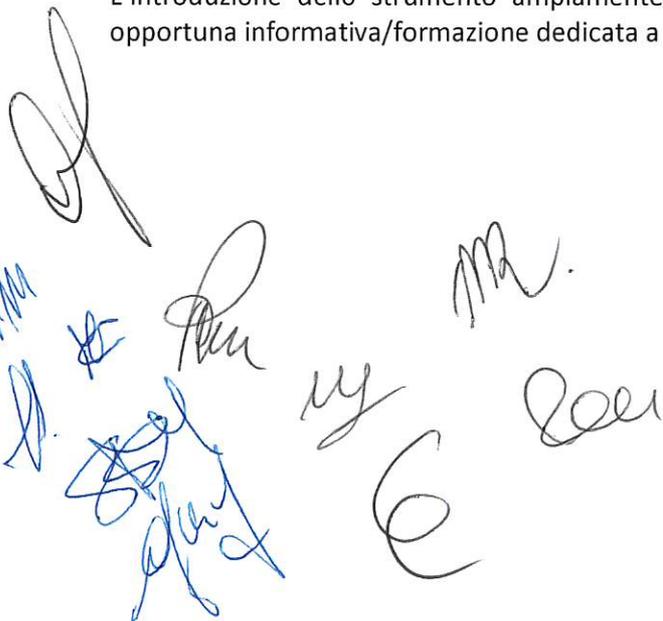
I dati trattati relativi agli eventi anomali registrati saranno conservati per un tempo fino a 90 giorni per consentire la correlazione di eventi anche distanti nel tempo e la ricostruzione a posteriori di eventuali fenomeni anomali e particolarmente complessi. Il periodo di conservazione dei dati potrà essere superato solo nei casi in cui permarranno le necessità di contrasto (esempio si prolungano gli effetti della minaccia e le conseguenti azioni di difesa) o a fronte di esigenze di tutela legale dell'Azienda o di richieste dell'Autorità Giudiziaria.

I soli soggetti aziendali che potranno avere accesso ai dati vengono identificati esclusivamente negli addetti alla Funzione *Cybersecurity*, e nelle persone del Direttore IT e dell'Amministratore Delegato, o persona da loro delegata, in conformità alla normativa privacy vigente.

In caso di un incidente informatico particolarmente rilevante sarà cura dell'Azienda informare le Rappresentanze Sindacali Unitarie sulla natura dell'evento e sulle azioni messe in atto per tutelare il patrimonio aziendale.

Con il presente accordo, per quanto di competenza, le Parti si danno atto di avere esperito le procedure previste dal suddetto art. 4 dello Statuto dei lavoratori e da ogni altra normativa applicabile. Eventuali aggiornamenti informatici dello strumento oggetto del presente accordo (o di eventuali strumenti analoghi non più invasivi in sostituzione di quello inizialmente adottato) o l'implementazione di nuove release dello stesso che non comportino un ampliamento degli usi e del trattamento dei dati, non saranno oggetto di ulteriori accordi. Rispetto ad esse la Società si impegna ad informare il sindacato. Per quanto previsto dall'art. 4, comma 3, della legge 300/1970 e dalla normativa privacy, contestualmente all'attivazione dei nuovi strumenti di sicurezza, la Società ha previsto la revisione del testo dell'informativa Privacy, che sarà reso disponibile a tutti i collaboratori e che specificherà la tipologia di trattamenti aggiuntivi introdotti dai nuovi strumenti di raccolta ed analisi dati ai fini della sicurezza e della tutela del patrimonio aziendale.

L'introduzione dello strumento ampiamente illustrato alle Organizzazioni Sindacali sarà oggetto di opportuna informativa/formazione dedicata a tutti i possessori di un personal computer aziendale.

A collection of handwritten signatures in black and blue ink, located in the bottom left corner of the page. The signatures are of various styles, some appearing to be initials or full names, and are scattered across the lower-left quadrant.

L'Azienda si impegna ad utilizzare i dati nel rispetto dei principi di proporzionalità tra i mezzi impiegati e i fini eseguiti. La Direzione Internal Audit ed il DPO vigilano sul corretto trattamento dei dati nel rispetto dei principi di cui al D.Lgs 196/03 (così come modificato dal D.Lgs 101/2018), al Regolamento privacy generale UE 2016/679 ("GDPR") e delle "Linee Guida di Gruppo sul trattamento dei dati personali" emesse dalla Società.

Assago (MI), 16 aprile 2019

Letto, confermato e sottoscritto.

Italiaonline S.p.A.



OO.SS.

