Policy per l'uso delle piattaforme digitali e videoconferenze

1. Premesse

In seguito all'emergenza sanitaria COVID-19, nell'ottica di limitare ogni contatto e promuovere le modalità di lavoro a distanza, l'Ordine degli Avvocati di Como adotta la presente policy per l'utilizzo di piattaforme digitali e altri strumenti informatici per lo svolgimento di riunioni, videoconferenze e udienze.

Il presente documento, pertanto, elenca i principali strumenti, ma anche le modalità informatiche e operative per lo svolgimento dell'attività ordinaria e richiama il proprio personale, dipendenti e collaboratori in ogni forma, ivi inclusi i mediatori, al rispetto della normativa privacy nell'utilizzo dei suddetti strumenti digitali.

2. Disciplina generale

E' opportuno rilevare e avere consapevolezza che ogni strumento digitale offre opportunità e anche rischi in quanto richiede di accedere ai nostri sistemi. Se, per esempio, ci si collega tramite web e senza scaricare i programmi, tendenzialmente le funzionalità dei prodotti sono ridotte al minimo, ma ovviamente risultano limitati anche i rischi di vulnerabilità del sistema, ivi incluso il rischio di effettuare il download e la relativa installazione di un virus.
Ogni funzionalità che i programmi richiedono e che l'utente fornisce acconsentendo apre una vulnerabilità nel sistema. Non essendo possibile per ogni utente destinare una macchina solo alle conference call, si richiede la massima attenzione nell'accettazione delle funzionalità del programma, con particolare riferimento per quelle di condivisione dati con altri programmi. Quando, per esempio, condividiamo lo schermo per mostrare a chi è nella call una presentazione o un documento stiamo aprendo una vulnerabilità nel sistema che potrebbe essere sfruttata per accessi illegittimi.

3. Piattaforme disponibili

Per lo svolgimento delle udienze è stato lo stesso Ministero della Giustizia a validare lo strumento di Skype for Buisness / Microsoft Teams, tuttavia lo stesso non avviene per le altre attività per le quali potrà quindi essere scelto il medesimo strumento o strumento diverso.

Sono inoltre disponibili le piattaforme di Zoom, Cisco Webex e SferaBit.
Attualmente l'Ordine degli Avvocati di Como e gli organismi collegati hanno deliberato di utilizzare la piattaforma **Zoom** per le sedute del Consiglio e degli altri organi collegiali dell'ordine e derivati (Commissioni e CPO) e **Sferabit** per la Mediazione.

Si sottolinea che il principio di pubblicità si applica alla maggior parte delle udienze. Al contrario, le sedute del Consiglio, eventuali convocazioni in Consiglio e gli incontri di mediazione sono riservati e sarà quindi necessario richiamare le parti agli obblighi di riservatezza e di non registrazione della teleconferenza, in qualsiasi forma attuata.
E' prevista in questi casi un richiamo ai profili privacy anche nella mail di invito per la partecipazione alla conference call.

4. Check list sicurezza informatica del computer scelto per lo smart working

Il primo passo, il più importante, è avere piena consapevolezza di quanto sia importante proteggere il computer sul quale si sta lavorando.

Sono almeno tre i livelli da tenere in considerazione: protezione del computer e della rete di casa, password e browser. Per ciascuna di queste categorie vedremo tutto quello che si dovrebbe fare per avere un livello di sicurezza minimo del sistema e di ogni dato trasferito sul web ed in rete.

1) Sicurezza del computer

□ E' stato installato un antivirus?
□ L'antivirus si aggiorna automaticamente ogni giorno?

Se non è stato ancora installato un antivirus oppure se si ha un programma scaduto che non si aggiorna più, bisogna prendere provvedimenti immediati.

□ E' installato un firewall?

Se si ha Windows, dalla versione 7 in poi, e se si naviga in internet usando un router a casa, non è necessario un programma firewall.

□ Windows (o Mac) è aggiornato e si aggiorna automaticamente e regolarmente?

Verificare che il servizio Windows Update sia attivo dal Pannello di Controllo.
Molti trascurano o dimenticano di aggiornare Windows con le patch (correzioni) che Microsoft distribuisce ogni settimana. Tali aggiornamenti sono importantissimi, molto più di quanto si possa immaginare.

□ Tieni aggiornati i programmi installati sul computer?

Il principio è lo stesso di cui sopra. Utilizzare un software non aggiornato all'ultima versione è un potenziale pericolo. Gli sviluppatori lavorano ogni giorno per aggiungere funzionalità ma anche e soprattutto per intervenire su falle di sicurezza.

IMPORTANTE
□ **Quando scarichi programmi, stai attento, nella procedura di installazione a non installare anche altri software "consigliati"?**

Purtroppo, molti programmi gratis sono accompagnati da sponsor, cosiddetti "crapware", sotto forma di programmi non richiesti che si installano automaticamente.

2) Sicurezza del browser

Il fatto che il computer sia protetto da virus e da intrusioni esterne non garantisce che la navigazione sia comunque sicura e privata.

In particolare:
□ Quando fai la login con password ad un sito, controlli sempre che l'indirizzo inizi con **https**?

HTTPS è il protocollo della connessione cifrata e si differenzia rispetto il normale http per il fatto che ogni dato trasmesso in https è crittografato. Questo significa che, anche volendo intercettare il traffico di rete, quanto viene scritto in https è illegibile per chiunque, compresi i gestori di quel sito.

IMPORTANTE
□ **Quando ti colleghi ad un sito da un computer non usato solo da te, esci sempre dall'account?**

Ricordare sempre di eseguire il logout di tutti gli account che si usano su un computer condiviso con altre persone, familiari compresi.

□ Conosci le basi delle truffe e le frodi online?

Sapere cosa sono il phishing, i malware e altri pericoli su internet è importante per stargli alla larga. Cerca le definizioni con qualsiasi motore di ricerca.
Da wikipedia: Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

3) Sicurezza delle password usate online (in caso di smart working davvero importante)

□ Usi password complesse?

Una degli errori più frequenti tra i navigatori su internet è di usare password semplici o che rimandano a fatti o eventi della vita personale.
Non utilizzare mai nomi propri, qualsiasi parola del vocabolario di qualsiasi lingua, numeri di telefono o date di nascita. Le password più sicure sono quelle irrecuperabili attraverso altre fonti.
Un buon metodo potrebbe essere quello di utilizzare le iniziali di una frase con senso logico, numeri e lettere maiuscole. Ad esempio: “E’ importante dotarsi di una (1) password sicura per la privacy” diventa “Eidd1psplp”.
NOTA: E’ buona norma utilizzare lettere maiuscole, numeri e caratteri speciali per aumentare le possibili combinazioni e, pertanto, innalzare il livello di sicurezza.

□ Usi password diverse per ogni sito?

Non bisogna mai riutilizzare la stessa combinazione e-mail e password in più servizi. Serve per evitare la violazione di ogni account personale senza fatica.