VERBALE DI ACCORDO SINDACALE

ex art. 4 Legge 20/05/1970 n. 300 e successive modificazioni

Oggi, 31 maggio in Roma, tra

Snaitech S.p.A., con sede legale in Milano, Piazza della Repubblica 32 (in seguito la Società) rappresentata da Lavinia Pupelli, Cecilia Ferro e Milena Giannetti, nonché il DPO Giorgio Aprile (qui di seguito anche "**Snaitech**" o la "**Società**")

E

le OO.SS. delle Segreterie Nazionali della **FISASCAT CISL**, nella persona di Marco Demurtas, della **UILTUCS**, nella persona di Emilio Fargnoli, della **SLC CGIL** nella persona Fabio Scurpa, della **FISMIC CONFSAL** nella persona di Silvio Battistini (qui di seguito, collettivamente, le "OO.SS.")

(qui di seguito, collettivamente, le "**Parti**")

Premesso che:

1. la Società ha la necessità di installare dei software per venire incontro e soddisfare le esigenze organizzative, di sicurezza informatica nonché di tutela del patrimonio aziendale e dei dati personali come prescritto anche dal D.Lgs. 30 giugno 2003, n. 196, dal Regolamento Europeo sulla Protezione dei Dati Personali (n. 2016/679) e dal D.Lgs. 10 agosto 2018, n. 101;

2. in particolare, per soddisfare le esigenze di cui sopra, la Società ha individuato i seguenti software: *UTM Sophos, Symantech DLP, SailPoint Identity IQ* e *Manage Engine LOG 360*;

3. i software di cui al precedente punto 2 saranno configurati dagli amministratori di sistema in modo da rispettare la normativa di riferimento, anche in materia di protezione dei dati personali, così da consentire ai dipendenti che usano gli strumenti aziendali il pieno rispetto della stessa;

4. il software ***UTM Sophos*** è un sistema di sicurezza della rete informatica aziendale che consente di registrare, mediante *file* di *log*, gli accessi negati alla rete aziendale e tutti gli accessi alla rete internet, da parte dei dipendenti. Tale registrazione dei dati avviene in maniera aggregata, ma qualora il sistema dovesse segnalare delle anomalie che possono risultare eventi reali e quindi oggetto di violazione, gli amministratori di sistema possono accedere ai dati di dettaglio risalendo al singolo dipendente a cui è riferibile l'anomalia stessa. Tali informazioni, aggregate, verranno conservate per sei mesi, di

dettaglio, per tre mesi; le Parti concordano che i dati raccolti non saranno utilizzati ai fini del controllo dell'attività lavorativa o comunque per finalità diverse o ulteriori da quelle indicate al punto 1., fatti salvi i controlli difensivi volti a sanzionare eventuali illeciti e, comunque, per esigenza di polizia o di giustizia.

5. il software ***Symantech DLP*** – unitamente al *plug-in Data Insight* – serve a prevenire fenomeni di *data breach.* Si tratta, infatti, di un *software* che identifica e localizza nella rete informatica aziendale i dati personali identificati dalla Società per conoscerne l'ubicazione e proteggerli di conseguenza. Una volta effettuata l'individuazione dei dati personali, il software registra eventuali tentativi di trasmissione degli stessi su canali non consentiti dalle regole aziendali, segnalandoli sia al dipendente mediante un *alert* diretto a quest'ultimo, sia ad una *console* centralizzata a cui hanno accesso solo gli amministratori di sistema. I dati e le informazioni di dettaglio così raccolte verranno conservate per sei mesi; l'informazione del numero e della tipologia di anomalie verrà conservata per un anno;

6. il software ***SailPoint Identity IQ*** è un sistema di profilazione dei dipendenti che consente di visualizzare, in modo centralizzato, gli accessi dei dipendenti alle piattaforme ed ai sistemi informatici aziendali che richiedono un *log-in*; il software consente di elaborare dei *report* da cui è possibile visualizzare i profili dei dipendenti a tutte le applicazioni configurate, senza registrare gli orari di accesso, rendendo anche possibile delle correlazioni per identificare i dipendenti che accedono a dati personali che sono fuori dal perimetro inerente alle mansioni affidate e ciò anche al fine di consentire e verificare la corretta assegnazione dei profili di accesso ai vari dipendenti. I dati e le informazioni di dettaglio così raccolte verranno conservate per sei mesi; l'informazione del numero e della tipologia di registrazioni verrà conservata per un anno;

7. il software ***Manage Engine LOG 360*** è un sistema che consente di tener traccia in tempo reale di tutti i *log* inerenti alle attività informatiche poste in essere esclusivamente dagli amministratori di sistema, mediante un sistema di *alert* che segnala le eventuali anomalie al ICT *Security Manager.* Tale software consente anche di elaborare dei *report* da cui è possibile visualizzare le operazioni svolte dai singoli amministratori di sistema. I dati e le informazioni di dettaglio così raccolte verranno conservate per sei mesi; l'informazione del numero e della tipologia di registrazioni relative a ciascun amministratore di sistema verrà conservata per un anno;

8. la Società nel corso del 2018 ha erogato a tutti i dipendenti una formazione specifica in materia del Trattamento dei dati personali, sia da un punto di vista normativo-giuridico sia da un punto di vista della sicurezza informatica.

Tutto ciò premesso si conviene e si stipula quanto segue:

1) Le Premesse fanno parte integrante del presente Accordo.
2) Le Parti si danno atto che l'installazione dei software *UTM Sophos, Symantech DLP, SailPoint Identity IQ* e *Manage Engine LOG 360* è necessaria per tutelare il patrimonio aziendale nonché per soddisfare le esigenze organizzative, di sicurezza informatica e di protezione dei dati personali, anche prescritte dal D.Lgs. 30 giugno 2003, n. 196, dal Regolamento Europeo sulla Protezione dei Dati Personali (n. 2016/679) e dal D.Lgs. 10 agosto 2018, n. 101;
3) Le Parti si danno altresì atto che le modalità di uso e le modalità di effettuazione dei controlli, relativi agli strumenti informatici oggetto del presente accordo sono quelle indicate ai punti 4, 5, 6 e 7 delle Premesse.
4) La Società si impegna a:
   a) informare i dipendenti circa le modalità di uso e le modalità di effettuazione dei controlli relativi agli strumenti informatici di cui sopra, ai sensi dell'art. 4, comma 3, Legge 20 maggio 1970, n. 300;
   b) assicurare che la raccolta dei dati e delle informazioni tramite i predetti strumenti informatici, nonché la gestione degli stessi da parte degli amministratori di sistema, avvenga nel rispetto delle disposizioni del D.Lgs. 30 giugno 2003, n. 196, del Regolamento UE in materia di protezione dei dati personali (Regolamento 2016/679), del D.Lgs. 10 agosto 2018, n. 101, nonché delle indicazioni tempo per tempo vigenti del Garante per la protezione dei Dati Personali.

Letto, confermato e sottoscritto.

per **Snaitech S.p.A.**

per **FISASCAT CISL**

per **UILTUCS**

per **SLC CGIL**

per **FISMIC CONFSAL**