VERBALE DI ACCORDO SINDACALE

EX ART. 4, COMMA 2, STAT. LAV.

Oggi, 2 Agosto, in Milano, presso **Marsh S.p.A.**, in Milano, Viale Bodio 33 si sono incontrati

Marsh S.p.A., rappresentata da Gianni Turci d'ora in avanti «la Società» o «Marsh»

e la **RSA FISAC/CGIL di Marsh S.p.A** (Fulvio Pavichievaz)

Le Parti, previa ampia ed esaustiva discussione hanno concluso il seguente accordo avente ad oggetto le modalità di controllo sull'utilizzo del personal computer, di internet, della posta elettronica, del telefono fisso e cellulare aziendali.

PREMESSO CHE

1. la Società fornisce in dotazione ai propri dipendenti al fine di un migliore svolgimento dell'attività lavorativa i seguenti beni: personal computer, internet e posta elettronica, ciascuno a seconda delle mansioni svolte dal dipendente assegnatario;
2. dovrà essere rispettata la disciplina dettata dal decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali", in particolare le "linee guida per posta elettronica e internet" deliberazione n. 13 del 1 marzo 2007, pubblicata sulla G.U. n. 58 del 10 marzo 2007
3. la Società si trova nella necessità di controllare il corretto utilizzo dei suddetti beni al fine di proteggere il proprio patrimonio e di evitare la diffusione di informazioni riservate non autorizzate nonché al fine di svolgere indagini difensive ovvero nel caso in cui sia necessario accertare, anche nel quadro della normativa di cui al D. Lgs. 8 giugno 2001, n. 231, comportamenti che possano costituire reato o che siano comunque illeciti posti in essere mediante l'utilizzo del personal computer, di Internet e della posta elettronica aziendale;
4. tutti i beni e/o servizi di cui sopra sono in grado di trattare dati riferibili direttamente o indirettamente al dipendente assegnatario e pertanto dal controllo effettuabile per le finalità di cui al punto 2 che precede, potrebbe derivare, direttamente o indirettamente, un trattamento di dati personali dei lavoratori;
5. è interesse primario della Società esercitare i controlli per le finalità di cui al punto 2 di cui sopra nel rispetto della libertà e dignità dei lavoratori, secondo le modalità stabilite dalla legge;
6. in base alle finalità di cui al punto 3 che precede è stata predisposta una procedura sull'utilizzo di internet, posta elettronica e telefoni aziendali (all. A) che indica:

    - le modalità di utilizzo di tutti i beni indicati al punto 1 che precede;
    - le finalità e le limitazioni dell'uso degli stessi beni;
    - le spiegazioni delle modalità di registrazione dei dati in entrata e in uscita;
    - la definizione di internet e posta elettronica e i limiti della loro utilizzazione;
    - gli scopi per cui è ammesso e quelli per cui è vietato l'uso degli strumenti di cui al punto 1 che precede;

- le modalità di controllo che verranno svolte dalla Società per verificare l'uso corretto degli strumenti di cui al punto 1 che precede, concessi in dotazione ai dipendenti;

Tutto ciò premesso,

le parti concordano quanto segue

1. PREMESSE

1.1. Le premesse costituiscono parte integrante del presente accordo

2. PROCEDURA PER L'USO DELL'INFORMATICA AZIENDALE

2.1. Le parti approvano la sezione 3, denominata "Controlli", della policy di cui all'All. A.

2.2. In particolare, fermo restando che le regole sull'uso degli strumenti e servizi di cui al punto 1 delle premesse non costituiscono oggetto del presente accordo e potranno essere modificate dall'azienda in ragione delle esigenze organizzative di tempo in tempo esistenti, previo incontro illustrativo con la RSA e successiva consegna della nuova procedura a tutti i lavoratori, la Società potrà esercitare il controllo sul rispetto delle modalità di utilizzo da parte dei dipendenti degli strumenti e servizi di cui al punto 1 delle premesse nei seguenti limiti e secondo le seguenti modalità concordemente con quanto stabilito nella suddetta sezione 3 della policy di cui all'All. A.

Controllo sul rispetto delle modalità di utilizzo di INTERNET e della POSTA ELETTRONICA

Marsh promuove ogni opportuna misura organizzativa, tecnologica e di sicurezza volta a prevenire il rischio di utilizzi indebiti che possono essere fonti di responsabilità, a "minimizzare" l'uso di dati riferibili ai lavoratori e a garantire la disponibilità e l'integrità dei sistemi informativi e dei dati; allo scopo, la Società ha adottato strumenti tecnici e organizzativi volti a prevenire trattamenti illeciti sui dati trattati con strumenti informatici, come illustrato nella presente procedura.

Marsh informa di aver adottato sistemi che evitano interferenze ingiustificate sui diritti e sulle libertà fondamentali dei lavoratori e dei soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata, nel rispetto del principio di pertinenza e non eccedenza, con esclusione di qualunque registrazione o monitoraggio sistematico e di analisi occulta.

Premesso che l'uso del PC aziendale, di INTERNET e dell'indirizzo di POSTA ELETTRONICA aziendale, attraverso le apparecchiature aziendali, è consentito solo per motivi di lavoro e nell'interesse esclusivo della SOCIETÀ, mentre ne è vietato l'uso personale, e che l'utilizzo dei sistemi informatici non conforme alle regole di cui alla presente Policy può comportare delle serie minacce alla sicurezza informatica e alla corretta conservazione dei dati essenziali per l'attività di Marsh nonché il rischio di sanzioni civili, amministrative e penali sia per Marsh sia per lo stesso lavoratore, la SOCIETÀ si riserva espressamente il diritto di esercitare controlli (ad esempio per fini di manutenzione, per esigenze di sicurezza, e/o per verificare il rispetto delle modalità di utilizzo da parte dei dipendenti degli strumenti informatici in dotazione, nonché al fine di prevenire e/o accertare la commissione di atti che possono costituire reati o comunque atti illeciti).

I controlli possono avvenire secondo due livelli, denominati rispettivamente "ordinario" e "straordinario", secondo le modalità di seguito descritte.

Controllo Ordinario

Il primo livello di controllo "ordinario" viene svolto in maniera anonima e in caso di elusione dei filtri preventivi preimpostati che riducono al minimo l'esigenza del controllo successivo. Il sistema di Firewall per l'accesso a siti Internet di contenuto illecito o comunque non attinente all'attività lavorativa nonché il sistema di filtraggio automatico delle mail (anti-spam, quarantena di files riconosciuti come non sicuri ecc.) possono infatti subire elusioni. In questo caso il sistema genera automaticamente degli avvisi di anomalia ("alert" relativi a, in via esemplificativa, scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) che vengono visualizzati dal personale IT. La finalità del controllo relativamente agli accessi a Internet è verificare se dai dati di connessione non risultino anomalie quali la violazione o l'elusione del sistema di blocco (Firewall) dei siti a contenuto illecito (es. siti a contenuto violento, discriminatorio, pornografico ecc.) o comunque non attinenti all'attività lavorativa . La finalità del controllo relativo alla posta elettronica è verificare che l'e-mail aziendale sia utilizzata in conformità con le regole di condotta stabilite nella presente Policy e quindi che non sia utilizzata per ricevere notifiche di messaggi da server esterni, non sicuri o comunque non attinenti all'attività lavorativa, per inviare a soggetti o indirizzi di posta elettronica non autorizzati informazioni e documenti riservati (es. invio di files a propri account di posta elettronica privati), per effettuare operazioni on-line non sicure e potenzialmente dannose non solo per Marsh ma per lo stesso lavoratore (es. acquisti su siti Internet, download di files audio/video in violazione della legge sul copyright ecc.).

In caso di avviso di anomalia, Marsh effettuerà un controllo anonimo sui dati aggregati riferito all'intera struttura aziendale oppure a sue aree, in modo da poter individuare l'area aziendale da richiamare al rispetto delle regole procedurali. Il controllo anonimo potrà concludersi con un avviso generalizzato relativo all'utilizzo anomalo di strumenti aziendali, con l'invito ad attenersi scrupolosamente alle istruzioni impartite a mezzo della presente procedura. Qualora il comportamento anomalo dovesse ripetersi o comunque nei casi di maggiore gravità (es. accesso a siti illegali o a contenuto discriminatorio o violento), Marsh potrà effettuare controlli su base individuale ("Controllo Straordinario").

Controllo Straordinario

Il secondo livello di controllo denominato "straordinario" viene attuato nei seguenti casi:

(a) nel caso in cui all'esito del controllo ordinario emergano comportamenti anomali ripetuti o comunque di particolare gravità (es. accesso a siti illegali o a contenuto discriminatorio o violento);

(b)nel caso vi sia l'esigenza di svolgere indagini di natura difensiva ovvero nel caso in cui sia necessario accertare, anche nel quadro della normativa di cui al D. Lgs. 8 giugno 2001, n. 231, comportamenti che possano costituire reato o che siano comunque illeciti o non conformi alla presente Policy e, in genere, ai regolamenti aziendali di Marsh, posti in essere mediante l'utilizzo del personal computer, di Internet e della posta elettronica aziendale.

Nei suddetti casi, Marsh potrà, per mezzo del proprio personale IT, previo coinvolgimento dell'HR Manager verificare il contenuto dei file presenti sui SERVER. A tal fine deve essere inoltrata apposita richiesta all'MGTI (MMC Global Technology Infrastructure) con sede a Londra da parte dell'IT locale di concerto con l'HR. Il controllo straordinario potrà avvenire, laddove la natura dell'indagine lo richieda, anche mediante accesso diretto al PC del dipendente che, su richiesta, dovrà consegnarlo al Responsabile IT.

Il controllo straordinario potrà altresì avvenire con la collaborazione di professionisti esterni (quali società di auditing, avvocati, consulenti informatici ecc.), mediante accesso al server e/o alla memoria di massa del computer dato in dotazione al dipendente. Marsh dovrà, in ogni caso, provvedere alla nomina di un responsabile del procedimento. In mancanza di nomina specifica il responsabile del procedimento sarà il Direttore del Personale. Il controllo straordinario non potrà avere ad oggetto un arco temporale eccedente i sei mesi precedenti la data in cui esso viene effettuato, salva la necessità di estendere l'indagine oltre tale periodo in ragione della natura del comportamento oggetto di indagine e/o in conseguenza di fatti emersi nel controllo relativo ai sei mesi precedenti la data dell'indagine. Del suddetto controllo, sarà redatto processo verbale che dovrà riportare la data di inizio dell'indagine, il motivo dell'indagine, una descrizione sintetica delle attività di indagine svolta, il relativo arco temporale, la data della chiusura dell'indagine, se la conclusione dell'indagine richiede o meno l'instaurazione di un procedimento disciplinare. Il verbale di indagine dovrà essere sottoscritto dal responsabile del procedimento. Qualora non sia necessaria l'instaurazione di un procedimento disciplinare, sarà conservata copia del verbale di indagine mentre i relativi documenti cartacei (es. stampa delle e-mail, stampa dei siti internet visitati ecc.) dovranno essere distrutti, salvo che tali documenti siano necessari al fine di difendere un diritto della Società nei confronti di soggetti diversi dal dipendente. Tale eventuale necessità di conservare i documenti cartacei d'indagine anche in mancanza di procedimenti disciplinari dovrà essere indicata e motivata nel verbale di indagine. Qualora si ritenga di dover instaurare un procedimento disciplinare, i documenti raccolti nel corso dell'indagine potranno essere conservati sia su sopporto informatico sia su supporto cartaceo, per il tempo necessario al fine di difendere i diritti di Marsh, connessi al procedimento disciplinare stesso e al suo esito.

In caso di indagine da effettuarsi per ordine di una Pubblica Autorità, potranno essere effettuati controlli anche al di fuori della suddetta procedura, secondo le modalità e con le procedure eventualmente prescritte dalla stessa Pubblica Autorità.

Resta inteso che entro 15 giorni dal completamento dell'indagine sarà data comunicazione alle RSA e al lavoratore.

Controlli sulla posta elettronica nell'ambito del programma BYOD (Bring Your Own Device)

Le regole stabilite per il controllo ordinario e il controllo straordinario sono applicabili, in relazione alle sole applicazioni aziendali, anche ai controlli della posta elettronica nell'ambito del programma BYOD.

Rappresentanti dei lavoratori nell'ambito del Controllo Straordinario

Le RSA avranno la facoltà di verificare i verbali di indagine secondo la procedura di seguito stabilita.

Con cadenza biennale, la Società, in apposito incontro da organizzarsi a richiesta delle RSA, fornirà una informativa sui controlli straordinari conclusi nei 24 mesi precedenti. A richiesta delle RSA, da inoltrarsi per iscritto (anche mediante e-mail) al Direttore del Personale, la Società dovrà concedere la consultazione dei verbali di indagine alle RSA. Entro sette giorni lavorativi dalla richiesta di consultazione la Società dovrà mettere a disposizione un locale e copia dei verbali di indagine relativi ai 24 mesi precedenti per la consultazione. Non è consentita la copia di alcun verbale di indagine, salvo diverso accordo con la Società. Nei sette giorni lavorativi successivi alla avvenuta consultazione le RSA potranno chiedere, per iscritto, un incontro con il responsabile del procedimento o i responsabili dei procedimenti che hanno sottoscritto i verbali di indagine oggetto di consultazione. Nella richiesta scritta di incontro dovranno essere sommariamente indicati i chiarimenti che le RSA intendono ottenere. Nei 7 giorni lavorativi successivi alla richiesta di incontro, la Società dovrà incontrare le RSA per fornire i chiarimenti che saranno richiesti. Decorsi 7 giorni lavorativi dalla data dell'incontro per i chiarimenti la procedura si intende esaurita senza alcun ulteriore obbligo per la Società. Con il consenso di entrambe le parti possono essere stabiliti di volta in volta, termini diversi, superiori o inferiori.

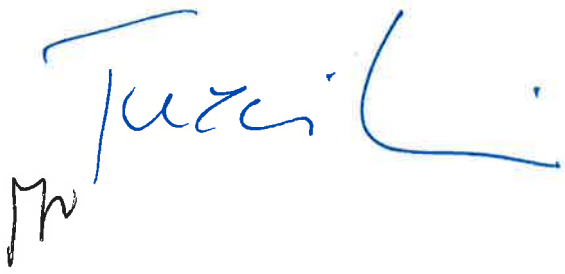
Tali modalità di Controllo Straordinario consentono di evitare che i controlli suddetti siano svolti con finalità di profilazione delle abitudini dei dipendenti o con finalità di controllo a distanza degli stessi.

2.3. Le informazioni di cui la Società venisse a conoscenza a seguito del controllo straordinario, non potranno essere utilizzate per accertamenti circa l'obbligo di diligenza del lavoratore, né per finalità di valutazione della prestazione, né per l'adozione di provvedimenti disciplinari, salvi i casi di dolo e/o colpa grave.

2.4. I dipendenti saranno informati del presente accordo sindacale mediante affissione in luogo accessibile a tutti e sarà consegnata copia della procedura di cui all. A. a ciascun dipendente.

Letto, confermato e sottoscritto

Marsh S.p.A. La RSA FISAC/CGIL



Si allega: All. A - **Procedura per l'uso dell'informatica aziendale** (Personal computer e altri dispositivi elettronici aziendali, internet e posta elettronica)