

## Verbale di Accordo

Addì 26 settembre 2011, presso la sede di UNINDUSTRIA – Confindustria Roma

*tra*

la soc. H3G S.p.A. (di seguito Azienda) assistita da UNINDUSTRIA – Confindustria Roma

*e*

la SLC CGIL, FISTEL CISL e UILCOM UIL nazionali e territoriali unitamente alle RSU

*premesso che:*

- l'Azienda, nell'esercizio della propria attività imprenditoriale, si è dotata di sistemi *hardware* e *software* per la gestione ed ottimizzazione di processi operativi di particolare rilevanza per il business aziendale e quindi per rispondere ad esigenze organizzative, produttive, nonché per rispondere ad esigenze di salvaguardia del proprio patrimonio aziendale e per la sicurezza del personale;
- l'Azienda si avvale anche di partner esterni abilitati agli accessi ai sistemi, di norma in qualità di responsabili del trattamento dei dati così come contrattualmente disciplinati. Tra i *partner* possono esserci figure in qualità di amministratori di sistema puntualmente censiti dall'Azienda;
- l'Azienda fornirà su richiesta dei lavoratori la lista aggiornata degli Amministratori di Sistema esterni.

Le Parti, per quanto in premessa, convengono quanto segue:

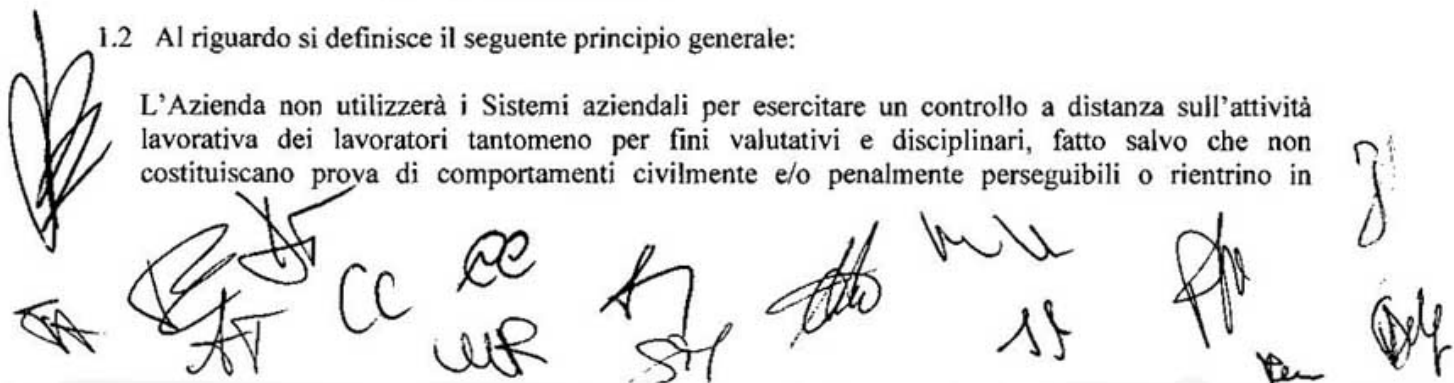
### 1. Oggetto

1.1 Con il presente accordo, in ottemperanza a quanto previsto dall'art 4, comma 2, della Legge 300/70, l'Azienda e le Rappresentanze Sindacali intendono definire quanto segue:

1. le finalità dell'utilizzo di sistemi informativi, *hardware* e *software*, di seguito "sistemi aziendali";
2. le modalità d'uso dei dati trattati dai Sistemi Aziendali;
3. la definizione dei soggetti preposti all'uso legittimo dei dati.

1.2 Al riguardo si definisce il seguente principio generale:

L'Azienda non utilizzerà i Sistemi aziendali per esercitare un controllo a distanza sull'attività lavorativa dei lavoratori tantomeno per fini valutativi e disciplinari, fatto salvo che non costituiscano prova di comportamenti civilmente e/o penalmente perseguibili o rientrino in



specifici obblighi di legge, ovvero nell'ambito di specifiche richieste avanzate dall'Autorità Giudiziaria o da un'Autorità Pubblica competente.

## **2. Sistemi di sicurezza e salvaguardia del patrimonio aziendale**

### **Finalità**

L'Azienda, per finalità di sicurezza e salvaguardia del patrimonio aziendale, si è dotata di sistemi di videosorveglianza e di controllo degli accessi per eseguire attività di monitoraggio ambientale.

### **Soggetto preposto**

All'interno della Direzione Security H3G esiste la figura del *Custodian Security*, unico possessore delle credenziali (*user e password*) per accedere ai sistemi di cui al presente paragrafo e che può altresì accedere legittimamente alle informazioni ivi contenute.

### **Sistemi specifici: 2.1) sistemi di videosorveglianza**

#### **2.1.1 descrizione**

Presso le sedi dell'Azienda sono installati sistemi di video sorveglianza, posizionati in luoghi che consentano il controllo del perimetro, dei varchi ascensori, degli ingressi principali/secondari/carrai, delle aree riservate (a titolo esemplificativo: CED), delle aree esposizioni, dei magazzini; i suddetti sistemi non inquadrano le postazioni e/o le aree di lavoro.

Le telecamere utilizzate sono di tipo analogico e di tipo over-IP con videoregistratori criptati.

Tutte le telecamere sono predisposte per effettuare registrazioni su dvr criptato situato in loco protetto/segregato, il cui accesso può avvenire esclusivamente mediante password.

Le immagini sono registrate e conservate in osservanza alla normativa e comunque per un periodo non superiore a 7 giorni.

I sistemi di videosorveglianza sono situati in tutte le sedi di lavoro.

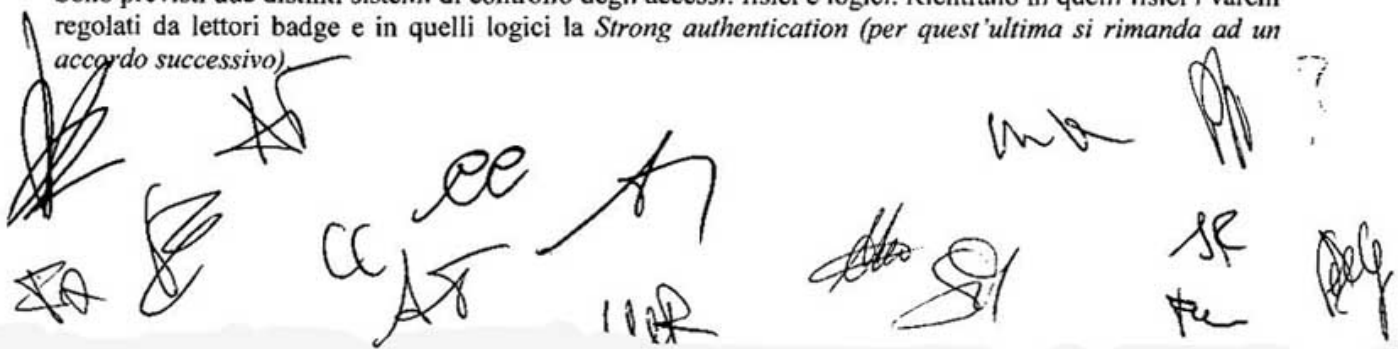
La presenza delle telecamere è segnalata in punti di massima visibilità da idonea informativa resa su apposita segnaletica.

In caso di riprese che possano produrre sanzioni disciplinari nei confronti del lavoratore l'Azienda informerà la RSU nei limiti e nel rispetto della legge vigente in materia di Privacy.

### **Sistemi specifici: 2.2) sistemi di controllo degli accessi**

#### **2.2.1 descrizione**

Sono previsti due distinti sistemi di controllo degli accessi: fisici e logici. Rientrano in quelli fisici i varchi regolati da lettori badge e in quelli logici la *Strong authentication* (per quest'ultima si rimanda ad un accordo successivo).

A collection of handwritten signatures and initials in black ink, scattered across the bottom of the page. Some are large and stylized, while others are smaller and more compact. They appear to be signatures of various individuals involved in the document's approval or creation.

I varchi regolati da lettori badge sono finalizzati ad evitare ingressi non autorizzati presso le sedi di lavoro dell'Azienda e di monitoraggio in caso di criticità e di tutela per le persone all'interno delle sedi. Tali sistemi sono posizionati all'ingresso dei luoghi di lavoro.

I dati relativi ai sistemi di accesso fisico sono acquisiti su un sistema centralizzato e conservati in appositi server ubicati all'interno di un ambiente riservato. Tali dati non possono essere utilizzati dall'Amministrazione del Personale per la rilevazione della presenza.

Il periodo di conservazione dei dati non potrà essere superiore a 2 mesi, fatte salve speciali esigenze di ulteriore conservazione nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria.

### **3. Sistemi per esigenze organizzative di gestione del personale (sistemi di rilevazione della presenza).**

#### **Finalità**

L'Azienda, per esigenze legate ad una ottimizzazione della gestione del personale, si è dotata di sistemi di rilevazione della presenza.

La presenza è rilevata appoggiando il badge sul lettore posizionato all'ingresso in prossimità del varco ascensore o su alcuni piani delle sedi. Vengono confermate le prassi in atto per quanto attiene smarrimento/furto ovvero dimenticanza del badge.

#### **Soggetto preposto**

I dati rilevati da questi lettori vengono inviati ad un server, da qui vengono trasferiti ogni ora al sistema aziendale per la rilevazione della presenza. Tali dati vengono conservati per un periodo non superiore a 10 anni. E' abilitato all'accesso per la consultazione dei dati il personale preposto nella Direzione *People Administration*.

### **4. Sistemi per la sicurezza degli apparati tecnici ed informatici.**

#### **Finalità**

L'Azienda per finalità di sicurezza aziendale si è dotata di sistemi logici che hanno l'obiettivo di rilevare e segnalare eventuali tentativi d'intrusione verso la rete aziendale dall'esterno verso l'interno e vice versa, e/o eventuali anomalie nel funzionamento dei server e degli apparati di rete, eventualmente dovuti anche a causa di un utilizzo improprio degli strumenti informatici da parte dei lavoratori.

L'attività di accesso remoto ai terminali dei dipendenti può avvenire esclusivamente per scopi di assistenza e/o di aggiornamento tecnico, nel rispetto delle norme in materia di dignità e riservatezza del lavoratore e segnalando allo stesso, l'intervento, in maniera preventiva.

La possibilità di svolgere attività e rilevare informazioni che anche indirettamente possano permettere un'accidentale forma di controllo, è subordinata alla verifica che essa venga svolta per la protezione del patrimonio aziendale, o a seguito di formale richiesta da parte delle autorità pubbliche competenti.

A collection of handwritten signatures and initials in black ink, located at the bottom of the page. The signatures are stylized and vary in complexity, including some that appear to be initials like 'CC', 'AT', 'UR', 'SP', 'FL', 'ST', 'PC', and others that are more elaborate and cursive.

### Soggetto preposto

I dati evidenziati attraverso questi sistemi sono conservati in appositi server per i periodi stabiliti dalla normativa e comunque per un periodo non superiore a 6 mesi; periodi maggiori di conservazione sono possibili esclusivamente in caso di contenziosi legali in atto o di richiesta da parte dell'Autorità Giudiziaria, ovvero qualora previsto dalla legge. E' abilitato all'accesso per la consultazione dei dati il personale preposto nella funzione IT Security della Direzione ICT.

## **5. Sistemi di gestione operativa**

### **Finalità**

L'Azienda per rispondere ad esigenze produttive ed organizzative si è dotata di sistemi appositi di gestione operativa per l'esercizio e l'ottimizzazione dei processi aziendali.

### **Sistemi specifici: 5.1) sistemi di gestione operativa**

Rientrano in questa fattispecie i sistemi di gestione del cliente (a titolo esemplificativo e non esaustivo People Soft, Egain, DCM, 3Sat, Irma, Cacs, ERP ecc) che hanno come obiettivo unicamente di:

- supportare gli Operatori nello svolgimento delle loro attività, rendendo disponibili in tempo reale informazioni e dati relativi al cliente, al fine di garantire efficacemente qualsiasi risoluzione dei problemi segnalati dal cliente stesso;
- dare visibilità agli Operatori delle informazioni di natura amministrativa del cliente al fine di poter gestire eventuali reclami o richieste del cliente;
- reportizzare e monitorare le varie attività attraverso idonei e innovativi sistemi per garantire che vengano svolte in linea con le esigenze qualitative dei servizi erogati alla clientela.
- individuare interventi formativi al fine di migliorare la qualità, la professionalità degli operatori, la correttezza dei processi e al fine di rispondere ai requisiti di qualità delle prestazioni rese.

L'estrazione dei dati, che potrà avvenire solo in modo aggregato tale da non permettere l'individuazione del singolo lavoratore, sarà utilizzata ai soli fini statistici e mirata al miglioramento del livello di servizio offerto alla clientela nonché al miglioramento dell'efficienza lavorativa e organizzativa e comunque non finalizzata al controllo a livello di singolo lavoratore. I dati a cui gli *account leader*, ovvero figure equivalenti, possono accedere saranno visibili solo in forma aggregata.

In particolare il livello di aggregazione su cui operare le estrazioni dei dati e la reportistica delle attività generate dai sistemi non deve essere inferiore al *pool*, e comunque mai inferiore a tre lavoratori qualora il *pool* sia ridotto.

Le parti si danno atto che anche le estrazioni dei dati, relative ad altri applicativi operanti nelle aree di Customer, dovranno essere effettuate solo in forma aggregata e mirate alle finalità di cui sopra.

I dati circa l'attività lavorativa svolta, desumibili dai sistemi in uso per le finalità tecniche, produttive e organizzative, non possono essere utilizzati a fini valutativi e disciplinari nei confronti del singolo lavoratore tranne che a seguito di formale richiesta da parte dell'Autorità Giudiziaria, o di un'Autorità Pubblica competente, anche a seguito di segnalazione formale del cliente alle stesse.

Handwritten signatures and initials at the bottom of the page, including a large signature on the left and several smaller ones on the right.

### Soggetto preposto

I dati contenuti in questi sistemi vengono conservati nel rispetto della normativa vigente e sono accessibili da personale preposto nella funzione IT Security della Direzione ICT. Gli eventuali accessi a questi dati saranno tracciati nel rispetto della normativa vigente.

### Commissione sul Controllo a Distanza (ex art. 4 Legge n. 300/1970)

La Commissione sul controllo a distanza, formata da due rappresentanti sindacali per ciascuna delle Organizzazioni Sindacali firmatarie il presente accordo e da rappresentanti aziendali, vigilerà sul rispetto del presente accordo e costituirà sede di informazione, monitoraggio, aggiornamento o modifiche sulle attuali modalità dei sistemi aziendali.

Resta inteso che RSU e Azienda organizzeranno incontri con cadenza trimestrale per l'esame di eventuali problematiche che dovessero insorgere nell'applicazione del presente accordo oppure, su richiesta della stessa RSU, per aggiornamenti periodici su nuovi sistemi aziendali.

L'azienda s'impegna infine a svolgere attività di sensibilizzazione nei confronti dei gestori/fruitori dei sistemi informatici per un utilizzo delle apparecchiature e dei sistemi coerenti con lo spirito e i contenuti delle intese sottoscritte.

Il presente accordo viene esteso a tutto il personale di 3lettronica Industriale SpA e di 3 Italia SpA. e ne sarà data ampia diffusione a tutti i lavoratori.

Letto, confermato e sottoscritto.

p. la UNINDUSTRIA - Confindustria Roma

p. la H3G.p.A.

p. la SLC - CGIL

p. la FISTEL - CISL

p. la UILCOM - UIL

p. le RSU

*[Handwritten signatures of representatives from UNINDUSTRIA, H3G.p.A., SLC - CGIL, FISTEL - CISL, UILCOM - UIL, and the RSU.]*