Addi' 10 maggio 2005 in Milano

Tra

IBM Italia S.p.A. (di seguito denominata IBM e/o Azienda) nelle persone di: Giuseppe Nicoletti, Umberto Zannier, Giuseppe Diodati,

e

il Coordinamento Nazionale delle RSU IBM Italia S.p.a.) nelle persone di Alfio Riboni, Valeria Bernardi, Giovanni Talpone,

si conviene quanto segue:

Premessa

IBM è una società all'avanguardia nel settore dell'Information Technology e dei servizi relativi alla clientela inserita nell'ambito di un articolato gruppo internazionale che svolge la propria attività per il tramite di hardware e software di diretta proprietà, di proprietà di varie controllanti, consociate ed affiliate e di clienti, utilizzando l'interconnettività garantita da un sistema di rete interaziendale, internazionale o tramite l'internet. Questi sistemi possono essere residenti in Italia o all'estero, indifferentemente regolati da una molteplicità di ordinamenti giuridici differenti; per tale motivo IBM Italia informerà delle previsioni del presente accordo le funzioni interne ed i soggetti esterni -anche esteri- che, per conto di IBM Italia, effettuino i trattamenti di dati, ove rientranti nel presente accordo.

Definizioni

a. Per "commissione sul controllo a distanza (CCD)" s'intende la commissione sindacale costituita da tre membri delle RSU designati dal Coordinamento a rappresentare i dipendenti IBM Italia per quanto concerne le tutele di cui al presente accordo; gli atti di tale commissione saranno validi quando sottoscritti da almeno due dei suoi componenti salvo diversa disposizione specificata nel presente accordo.

b. Per "responsabile aziendale dei rapporti con CCD (RARC)" s'intende l'incaricato nel tempo nominato dall'azienda e presentato per iscritto alla CCD ai fini della gestione del presente accordo.

c. Con la parola inglese "log" s'intende qualsiasi registrazione delle attività elaborative compiute da un'applicazione che permette di ricostruire le operazioni svolte connesse con il codice dell'utente che ha operato.

1. Le RSU prendono atto che:

a) dato il particolare settore produttivo in cui l'azienda opera, e cioè l'elaborazione elettronica dei dati, l'utilizzo di strumentazione informatica costituisce un elemento fondamentale su cui si basa l'attività economica aziendale ed indispensabile per lo svolgimento di essa;

b) l'azienda, anche in conformità agli obblighi derivanti dalla normativa vigente, ha attribuito ai fini di sicurezza a ciascun dipendente un codice identificativo personale per l'utilizzazione dell'elaboratore.

*

2. Stante quanto precede, il presente accordo costituisce l'adempimento delle previsioni dell'art. 4, comma 2, della L. 300/70. Esulano da esso i trattamenti imposti da norme di legge, nazionali ed internazionali, nonché i trattamenti difensivi derivanti da comportamenti penalmente sanzionati.

a. (Dichiarazione di principio) IBM conferma che intende utilizzare i dati relativi agli accessi del personale ai propri sistemi, applicazioni, programmi, dati e transazioni per motivi di sicurezza, corretta gestione degli stessi dati e informazioni, trattamenti statistici sui tool aziendali aggiornati direttamente dagli utenti con dati di loro pertinenza (ad es. PBC, IDP, note spese, cartellino orologio, etc.), corretta gestione delle risorse informatiche e per le statistiche d'uso relative ai sistemi informatici aziendali nonché per le attività relative a modifiche tecniche/operative e per l'addebito dei costi relativi all'utilizzo dei server ai reparti; IBM ribadisce inoltre, che i dati relativi non saranno in alcun caso utilizzati per controlli inerenti all'attività svolta dai dipendenti, né per fini diversi da quelli dichiarati nel presente accordo;

b. (Inventario delle applicazioni) L'azienda renderà e manterrà accessibile alla CCD un elenco aggiornato di tutte le applicazioni utilizzate dai dipendenti di IBM Italia; ogni voce conterrà:

- il nome dell'applicazione;

- lo scopo dell'applicazione stessa;
- il nominativo dell'amministratore dell'applicazione;
- gli ambienti informatici in cui è operativa;
- i centri e i Paesi in cui viene eseguita;
- i processi aziendali che utilizzano l'applicazione;
- la presenza sui log dell'identificativo utente;
- i centri e i Paesi in cui i dati e i log sono conservati, incluso le copie di salvataggio e sicurezza (backup);
- i criteri con cui i dati e i log sono conservati nel tempo o cancellati;
- l'eventuale disattivazione, cambio di versione (release), migrazione ed altra applicazione sostitutiva, spostamento ad altri centri e/o Paesi o adozione di altre forme, anche parziali, di esternalizzazione;
- informazioni particolari di cui agli articoli successivi.

Ogni qualvolta si rendesse necessario un aggiornamento intermedio, IBM ne darà comunicazione alla CCD segnalando l'aggiornamento della lista di cui sopra. In tale occasione la CCD potrà richiedere ad IBM informazioni in merito al funzionamento delle predette applicazioni nei limiti di quanto previsto dal presente accordo.

Qualora la CCD individuasse nella lista di cui sopra applicazioni con specificità di trattamento dei dati che richiedano un esame approfondito, lo comunicherà al RARC che avvierà tempestivamente il citato esame.

Qualora la CCD individuasse invece applicazioni con specificità di trattamento dei dati che esulino dagli accordi sottoscritti, IBM, su richiesta della CCD medesima, ove le esigenze tecniche e produttive aziendali lo consentano, valuterà se sospendere o disabilitare l'applicazione fintanto che le parti sottoscriventi il presente accordo non avranno trovato una soluzione negoziale. In detta richiesta, la CCD dovrà illustrare per iscritto le motivazioni per le quali le applicazioni in oggetto non possono essere fatte rientrare nel presente accordo.

c. (Evoluzione tecnologica) Qualora, grazie all'evoluzione tecnologica, si rendessero disponibili soluzioni tecniche in grado di assicurare una maggiore affidabilità e sicurezza in relazione alle tutele di cui al presente accordo, IBM valuterà

la possibilità di introdurle nel proprio sistema informatico. La CCD potrà in ogni tempo segnalare ad IBM quali soluzioni tecnologiche ritiene tecnicamente e ragionevolmente suscettibili di applicazione ai sistemi informatici IBM.

d. (Gestione dei sistemi di cifratura). Per ciascuna applicazione presente nell'elenco di cui al punto 2b e dotata di sistemi di cifratura, viene preventivamente stilato da IBM e successivamente aggiornato quando necessario, un documento operativo contenente:

- la descrizione della soluzione tecnologica adottata specificando se essa opera sulla stazione di lavoro dell'utente o su altro dispositivo periferico, o all'ingresso della unità centrale di elaborazione, o all'uscita di questa, o comunque in modo che risulti chiaramente il flusso dei dati personali dei dipendenti nei sistemi e i tratti di tale flusso in cui tali dati sono cifrati;
- la tipologia dei tentativi di accesso non autorizzato al sistema per i quali i sistemi di sicurezza danno all'utente risposta negativa, dando origine a registrazioni di log non cifrate.

Alla data di stipula del presente accordo, gli unici sistemi di cifratura operativi sono descritti negli allegati "A" e "B". Le definizioni dei sistemi di cifratura sono rispettivamente contenute negli allegati "D" ed "E".

e. (Riservatezza). Tutte le informazioni oggetto del presente accordo costituiscono patrimonio aziendale IBM e sono tutelate dalle norme sulla riservatezza previste dall'ordinamento giuridico, nonché dalle disposizioni aziendali IBM in materia (Codice Disciplinare, BCG, direttive, circolari ed istruzioni interne, etc.) ove non in contrasto con il medesimo ordinamento giuridico. La CCD manterrà la più completa riservatezza sulle informazioni di cui venisse a conoscenza per effetto dell'applicazione del presente accordo: in particolare, la CCD non rivelerà e non divulgherà, in qualsiasi modo, sia all'interno, sia all'esterno dell'azienda, informazioni inerenti alla società, alle sue controllate e/o clienti, né relative ai prodotti hardware e software di proprietà delle aziende del gruppo o di clienti, salvi i diritti di legge.

f) (Controllo e uso dei dati di accesso e di utilizzo dei sistemi e dei log). Il RARC, a fronte di gravi motivazioni o per necessità di sicurezza ed esclusivamente sulle

applicazioni già presenti nella lista di cui al punto 2b, e solamente in riferimento ai dati contenuti in detta lista, nonché nel rispetto dei principi di cui al presente accordo, comunicherà preventivamente, in forma scritta, alla CCD l'esigenza di effettuare interrogazioni, decifrazioni, analisi, correlazioni e controlli in genere sui dati riguardanti gli accessi e l'utilizzo dei sistemi da parte dei dipendenti. Detta comunicazione dovrà contenere la motivazione o la necessità di sicurezza che rende inderogabile l'esigenza di effettuare i predetti trattamenti; dovrà altresì specificare il trattamento che si intende effettuare e l'applicazione o le applicazioni coinvolte, nonché se il trattamento per conto di IBM Italia debba essere effettuato in un Paese estero o da un'altra azienda, e se i dati o le elaborazioni risultanti dal trattamento dovranno essere trasmesse ad altri soggetti.

Nel caso in cui la CCD ritenga non sussistere le motivazioni od esigenze di sicurezza comunicate dal RARC o che comunque il trattamento comunicato non sia rispettoso dei principi di cui al presente accordo e ritenga tale trattamento in violazione della normativa sul controllo a distanza, la stessa CCD comunicherà per iscritto, al RARC il proprio dissenso.

Viceversa nel caso di effettuazione del trattamento comunicato dal RARC, la CCD ha diritto di partecipare a tutte le operazioni in cui il trattamento stesso si articola, al fine di garantire la corrispondenza con i principi del presente accordo, nonché di verificarne la stretta strumentalità con la motivazione o l'esigenza di sicurezza comunicata. Il RARC dovrà fornire tutti gli strumenti tecnici e conoscitivi per mettere in grado la CCD di svolgere il proprio ruolo.

Il trattamento potrà durare al massimo quindici giorni lavorativi consecutivi.

Qualora emergano responsabilità a carico di un dipendente si applicheranno le procedure disciplinari previste dalla legge o dalla contrattazione collettiva applicabile. Effettuata la contestazione disciplinare, immediatamente dopo, il materiale derivante dalla procedura di controllo sarà messo a disposizione del dipendente ai fini dell'esercizio del diritto di difesa.

Il materiale derivante dalla procedura di controllo, in caso di esito negativo della stessa, verrà distrutto.

g. (Verbali) Al termine delle operazioni di cui al punto che precede, verrà redatto un verbale contenente le seguenti informazioni:

le motivazioni dell'indagine;

l'elenco dei sistemi acceduti;

le operazioni fondamentali compiute su detti sistemi;

la data e il luogo in cui l'indagine è stata compiuta;

i nominativi delle persone presenti alle operazioni;

l'elenco dei record analizzati per ciascuna applicazione, con l'indicazione dei dati identificativi del dipendente che ha operato su di essi;

l'eventuale dichiarazione dell'intervenuta distruzione del materiale prodotto del trattamento;

la sottoscrizione delle persone presenti.

h) (Accesso a sedi e aree riservate - Gestione delle spese telefoniche). Ai fini delle tutele di cui al presente accordo l'accesso a sedi e aree riservate e la gestione delle spese telefoniche effettuati dai dipendenti sono regolati rispettivamente agli allegati "B" e "C" del presente accordo, di cui costituiscono parte integrante. L'allegato "C" (gestione delle spese telefoniche) sostituisce l'accordo 17.12.1993-parte B di pari oggetto.

i. (Spesa) Le spese sostenute dai rappresentanti delle RSU in CCD per la partecipazione alle operazioni sopraccitate saranno rimborsate secondo la prassi aziendale vigente. I rappresentanti della RSU in CCD esporranno permessi sindacali retribuiti a carico del Coordinamento per il tempo dedicato alle operazioni.

3. IBM opererà rispettando il presente accordo e si impegna a trasmetterlo alle funzioni che effettueranno controlli. A tali fini, con riferimento ai trattamenti di dati effettuati per conto di IBM Italia da soggetti esterni, IBM Italia non richiederà a detti soggetti trattamenti in contrasto con il presente accordo e distruggerà, immediatamente, risultati di analisi in contrasto con il presente accordo eventualmente pervenuti in suo possesso.

4. Gli accordi aziendali del 23.2.1982, 2.10.1985, 23.4.1991 si intendono integralmente sostituiti dal presente accordo.

5. Le parti, a dodici mesi a far data dal presente accordo, si incontreranno per una verifica dell'applicazione.

6. L'efficacia della procedura di cui alla clausola 2f del presente accordo (Controllo e uso dei dati di accesso e di utilizzo dei sistemi e dei log) è condizionata alla creazione dell'Inventario delle applicazioni di cui alla clausola 2b.

Letto confermato e sottoscritto

p. la Direzione

p. il Coordinamento R.S.U.

Allegato A

Il Sistema z/OS ex MVS ex OS/390 è un sistema coperto da cifratura come da allegato "D".

Allegato B - Aree e sedi riservate.

Tutte le applicazioni che gestiscono gli accessi alle sedi e alle aree riservate devono essere inserite nell'elenco delle applicazioni previsto dall'accordo.

Fatto salvo il vigente accordo 11.3.1983 che regola anche le modalita' di introduzione di nuove aree riservate nelle sedi IBM, i sistemi di controllo degli accessi sono coperti da cifratura a sistema CASIRUSCO, descritto nell'allegato "E".

Per tentativo d'accesso non autorizzato al sistema si intende tanto l'accesso alla applicazione quanto l'accesso all'area riservata.

Allegato C - Gestione delle spese telefoniche.

Modalità per la gestione di:

1. telefonate per servizio;
2. telefonate per ragioni diverse da quelle di servizio.

mediante l'utilizzo di apparecchi sia di telefonia fissa, sia di telefonia mobile.

TELEFONATE DI SERVIZIO

Ad ogni dipendente viene assegnato un telefono con linea abilitata secondo le necessità di servizio (interno, locale urbano, interurbano, europeo, intercontinentale).

La funzione/reparto riceverà periodicamente il consuntivo della spesa e, a richiesta, potrà avere la lista dei costi sostenuti. Tale lista conterrà:

numero chiamante;

numero chiamato con indicazione del totale della spesa sostenuta e mascheratura delle ultime tre cifre.

La registrazione avviene al solo scopo di consentire all'azienda un adeguato controllo dei costi.

Non verranno evidenziate le chiamate verso numeri collegati a linee affittate (no-cost).

Ogni singolo dipendente riceverà copia della stessa lista richiesta dalla Funzione/Reparto, con i costi sostenuti per telefonate di servizio da esso stesso originate.

La società si impegna ad utilizzare i dati di cui sopra, ed oggetto di registrazione, al solo ed esclusivo scopo di procedere agli addebiti di reparto sopra descritti e comunque nel pieno rispetto del presente accordo.

Eventuali registrazioni delle telefonate (per esempio, per la verifica della qualità del servizio) possono essere effettuate solo dopo aver richiesto autorizzazione esplicita della registrazione a tutti gli interlocutori.

TELEFONATE DIVERSE DA QUELLE DI SERVIZIO

Il dipendente può utilizzare qualunque telefono fisso e/o mobile assegnato in comodato d'uso gratuito; al dipendente viene assegnato un codice segreto che, unito al suo numero telefonico,o codice personale, o altro sistema di cifratura, gli consenta di accedere alla linea urbana esterna.

Verranno registrati:

il codice personale;
il numero chiamante;
il numero chiamato con mascheratura delle ultime tre cifre;
il giorno, l'ora, il numero di scatti e l'importo da addebitare a cedolino.

INFORMAZIONE AL DIPENDENTE

Il dipendente riceverà mensilmente una comunicazione con dettaglio di tutte le proprie chiamate a mezzo posta elettronica se utente della stessa, oppure a cura del capo diretto se non utente; in tale comunicazione sarà indicata la spesa sostenuta nel mese, la spesa alla data e che verrà, successivamente, addebitata sul cedolino retribuzione.

La società distruggerà i dati oggetto di questa comunicazione entro 90 giorni.

Le registrazioni verranno utilizzate al solo fine di consentire l'addebito delle telefonate personali e comunque nel pieno rispetto del presente accordo.

In caso di necessità, il dipendente potrà richiedere l'assegnazione di un nuovo codice segreto.

Tutte le applicazioni di gestione delle telefonate devono essere presenti nell'inventario delle applicazioni previsto dall'accordo.

Dovrà essere garantita ad ogni dipendente la possibilità di utilizzare un telefono pubblico e a questo scopo, IBM manterrà installati, presso ogni ubicazione, un adeguato numero di telefoni pubblici, se possibile, a scheda.

Allegato D - Definizione del sistema protetto da cifratura di cui all'All. "A".

Per tutte le applicazioni, le transazioni, le procedure e gli ambienti interattivi del sistema di cui all'All. "A", l'accesso avverrà mediante codice individuale.

Il codice individuale, gli indirizzi e gli altri dati che consentono di determinare la postazione di chi accede, verranno crittografati già nelle memorie di sistema, in modo che tutte le registrazioni permanenti (record SMF) contengano i suddetti dati solo in forma crittografata.

Tutti i tentativi di accesso non autorizzato al sistema (password invalida o userid revocato), la cui tipologia deve essere riportata nell'inventario delle applicazioni, e per i quali i sistemi di sicurezza danno all'utente risposta negativa, non saranno cifrati.

Il sistema di cifratura, attivato congiuntamente dal RARC e dalla CCD, determina la generazione in modo 'random' di una coppia di chiavi asimmetriche RSA (Rivest-Shamir-Adleman), una di cifratura (chiave pubblica) e una di decifrazione (chiave privata); la prima viene memorizzata e distribuita su tutti i sistemi ove è attiva la crittografia mentre la seconda non viene memorizzata e prima della sua immediata distruzione viene scomposta in due meta' ; una di dette meta' viene assegnata al RARC e l'altra al CCD.

Le modalità operative di questa cifratura saranno definite in un documento da allegare all'inventario delle applicazioni.

La creazione di una nuova coppia di chiavi di cifratura / decifrazione dovrà avvenire ogni 6 mesi dalla creazione delle precedenti. Le vecchie versioni delle chiavi dovranno essere mantenute da ciascuna delle parti per un periodo di 12 mesi.

Il RARC renderà disponibile alla CCD gli strumenti che consentano di verificare che il sistema di cifratura / decifrazione non possa venire manomesso o eluso.

Allegato E - Definizione del sistema protetto da cifratura di cui all'All. "B".

Per tutte le applicazioni (o sistemi), di cui all'All. "B", l'accesso avverrà mediante codice individuale.

Il codice individuale, e gli altri dati che consentono di individuare l'accesso, verranno rilevati dagli appositi lettori che trasmetteranno le informazioni, in codice macchina, ad un Host security risk che a sua volta le trasmetterà ad una macchina crittografatrice tramite un cavo allarmato.

Tutti i tentativi di accesso non autorizzato, per i quali i sistemi di sicurezza danno all'utente risposta negativa, non saranno cifrati.

Il sistema di cifratura, attivato congiuntamente dal RARC e dalla CCD, determina la generazione in modo 'random' di una coppia di chiavi asimmetriche RSA (Rivest-Shamir-Adleman), una di cifratura (chiave pubblica) e una di decifrazione (chiave privata); la prima viene memorizzata e distribuita su tutti i sistemi ove e' attiva la crittografia mentre la seconda non viene memorizzata e prima della sua immediata distruzione viene scomposta in due meta' ; una di dette meta' viene assegnata al RARC e l'altra al CCD.

Le modalità operative di questa cifratura saranno definite in un documento da allegare all'inventario delle applicazioni.

La creazione di una nuova coppia di chiavi di cifratura / decifrazione dovrà avvenire ogni 6 mesi dalla creazione delle precedenti. Le vecchie versioni delle chiavi dovranno essere mantenute da ciascuna delle parti per un periodo di 12 mesi.

Il RARC renderà disponibile alla CCD gli strumenti che consentano di verificare che il sistema di cifratura / decifrazione non possa venire manomesso o eluso.