*Verbale di Accordo*
*ai sensi dell'art.4 Legge n.300/70*

Addì 03/01/2024*, in Roma*
*tra*
Telecontact Center S.p.A.

*e*

*le Organizzazioni Sindacali SLC-CGIL, FISTel-CISL, UILCom-UIL, UGL Telecomunicazioni, unitamente alle RSU*

*Premesso che*

- in data 4 dicembre 2019 è stato sottoscritto da TIM S.p.A. e dalle OO.SS. SLC-CGIL, FISTel-CISL, UILCom-UIL, UGL Telecomunicazioni unitamente al Coordinamento Nazionale RSU l'Accordo Frodi interne relativo al sistema Monitoring & Detection che consente di sistematizzare e coordinare le attività di prevenzione e contrasto delle frodi interne, con lo scopo di prevenire reati e comportamenti illeciti;

- Il Gruppo TIM adotta un Processo di Enterprise Risk Management (c.d. ERM) che consente di identificare e valutare quantitativamente i rischi che incidono sugli obiettivi di business e gestirli in modo omogeneo ed integrato. Il rischio Frode rientra nel perimetro di analisi del processo ERM ed è gestito dalla funzione antifrode della Capogruppo tramite il processo di Fraud Risk Assessment. Tale processo costituito da una attività di assessment, a cui contribuisce Telecontact Center in coordinamento con la funzione antifrode della Capogruppo, è volto a mappare ed analizzare gli scenari di frode/abuso, i relativi controlli in essere ed eventualmente individuare le contromisure da implementare per gestire adeguatamente i rischi rilevati.

- alla luce delle risultanze di questo assessment, nonché della ricorrenza di episodi di frode interna riscontrati, per i quali sono state avviate le azioni di tutela previste, Telecontact Center ha assegnato il compito di garantire il coordinamento delle attività di prevenzione e contrasto delle frodi interne, alla Funzione *antifrode della Capogruppo.*

- ai sensi dell'art. 4, legge n. 300/1970, gli impianti audiovisivi e gli altri strumenti dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati anche per la tutela del patrimonio aziendale, previo accordo sindacale.

*Tutto ciò premesso si conviene quanto segue:*

**1. Adozione ed implementazione del sistema Monitoring & Detection**

1.1. Per l'effettuazione delle attività di monitoring & detection sarà adottato un sistema informatico antifrodi secondo i criteri di legittimità di seguito riportati, a tutela dei diritti del lavoratore:

- controlli ex-post e non in tempo reale (rilevazione delle informazioni su attività non modificabili, non effettuati in real time o near real time);

- rispetto dei principi di specificità e temporaneità del controllo;

- fondato sospetto dell'esistenza e reiterazione di un illecito;

- rispetto dei principi applicabili al trattamento dei dati personali in conformità al Regolamento UE 2016/679: liceità, correttezza e trasparenza, pertinenza, e, minimizzazione.

1.2. Il sistema effettuerà, a tutela del patrimonio aziendale, la rilevazione delle informazioni relative a concentrazioni di operazioni anomale che facciano ipotizzare gravi illeciti, anche con riferimento ai reati ricadenti nel perimetro del d.lgs. 231/2001, in modo automatico e permettendo accessi solo a dati pseudonimizzati.

1.3. In una prima fase, l'analisi delle transazioni concluse nei sistemi utilizzati nei differenti processi di business presidiati (a titolo esemplificativo e non esaustivo: sistemi per la gestione dei buoni d'ordine e delle "entrate merci", di commercializzazione, di archiviazione del traffico fonia e dati, etc...) sarà effettuata in modalità automatica senza procedere ad identificazione del soggetto cui è riferita l'esecuzione della transazione. In questa fase saranno mascherati i dati identificativi dei singoli soggetti e l'analisi sarà finalizzata all'individuazione di concentrazioni di eventi anomali, rilevatori di possibili condotte illecite.

1.4. Eventuali successivi approfondimenti delle transazioni (quali ad esempio, l'analisi sulla ripetitività dell'evento, l'individuazione di possibile schema di frode, la verifica di altri eventuali fenomeni anomali correlati a quello rilevato) si svolgeranno sempre in modalità "automatica" o ricorrendo al personale della funzione antifrode competente, evitando l'adozione di controlli massivi e indiscriminati su dati non pseudonimizzati.

1.5. Solo nel caso in cui l'esito dei predetti approfondimenti confermasse il sospetto dell'esistenza e reiterazione del comportamento illecito, la funzione antifrode competente chiederà all'amministratore del sistema interessato di rendere intellegibili le informazioni concernenti l'evento anomalo, ivi compresa la matricola cui tale operazione è riconducibile, al fine di consolidare l'esito delle azioni a tutela aziendale ed adottare le opportune iniziative di coinvolgimento di ogni funzione aziendale competente.

**2. Soggetti legittimati all'accesso dei dati**

2.1. Gli amministratori di sistema, appositamente designati nell'ambito della funzione IT di TIM ai sensi del Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 in materia di "Misure ed accorgimenti prescritti ai titolari di trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", sono identificati come unici soggetti autorizzati ad accedere al tracciamento completo dei dati individuali dei singoli operatori e ad eseguire il relativo trattamento all'esclusivo scopo di rendere accessibili agli operatori della funzione antifrode competente solo i dati oggetto di approfondimenti.

2.2. Gli amministratori di sistema sono tenuti al rispetto delle policy, delle procedure e delle disposizioni aziendali in materia di sicurezza e di gestione degli accessi ai sistemi informatici.

**3. Utilizzo dei dati**

3.1. I dati non potranno essere utilizzati per verificare il corretto adempimento della prestazione lavorativa e pertanto non potranno essere diffusi né utilizzati in altri ambiti aziendali né trattati ai fini disciplinari salvo il caso in cui emergessero evidenze di comportamenti illeciti.

**4. Conservazione dei dati**

4.1. I dati sottoposti alle analisi effettuate in modalità automatica senza procedere ad identificazione del soggetto cui è riferita (cfr. 1.2) sono conservati per 15 mesi, al fine di individuare fenomeni ricorrenti e sviluppare controlli almeno annuali.

4.2. La conservazione dei dati individuali in chiaro, acquisiti dagli operatori della funzione antifrode competente secondo i criteri sopra riportati, avverrà per un periodo non superiore a quello strettamente necessario alla conclusione dell'attività di accertamento dei fatti; gli stessi saranno immediatamente cancellati in caso di esito negativo delle verifiche.

4.3 Nel caso in cui i dati evidenzino l'esistenza di una possibile frode, gli stessi saranno conservati per il tempo necessario alla conclusione delle azioni avviate a tutela della società e del relativo iter giudiziario o amministrativo.

**5. Informativa**

5.1. In coerenza con la normativa vigente, sarà data ai lavoratori adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli. I dati oggetto della presente intesa saranno trattati e conservati in coerenza con i punti precedenti e secondo i principi stabiliti dalla normativa sulla protezione dei dati personali, in particolare con riferimento al Regolamento UE 2016/679 (General Data Protection Regulation).

**6. Verifiche**

6.1. Le Parti si danno atto che si incontreranno entro sei mesi dall'avvio operativo del sistema oggetto del presente accordo al fine di monitorare l'andamento del processo ed eventuali episodi di frode emersi.

6.2. Eventuali modifiche del sistema derivanti dall'evoluzione tecnologica digitale, che consentano di raggiungere le medesime finalità, saranno oggetto di verifica fra le parti.

Letto, confermato e sottoscritto in via telematica.

per Telecontact Center S.p.A.

per SLC-CGIL

per FISTel-CISL

per UILCOM-UIL

per UGL Telecomunicazioni

| SEGRETERIE NAZIONALI | FAVOREVOLE | CONTRARIO |
|---|---|---|
| **SLC-CGIL** | **SI** | |
| **FISTel-CISL** | **SI** | |
| **UILCom-UIL** | **SI** | |
| **UGL-Telecomunicazioni** | **SI** | |

## Estrazione 3 gennaio 2024

| Ora di completamento | Nome | Vuoi sottoscrivere l'accordo Monitoring & Detection-Frodi Interne TCC di cui è stata data lettura in data odierna fra l'Azienda e le Organizzazioni Sindacali e RSU? |
|---|---|---|
| 1/3/24 11:46:30 | Anna Carlino | SI |
| 1/3/24 11:46:31 | Francesco Buttazzo | SI |
| 1/3/24 11:46:42 | Daniele Postorino | SI |
| 1/3/24 11:46:43 | Angela Sinopoli | SI |
| 1/3/24 11:46:46 | Cesidio D'Amore | SI |
| 1/3/24 11:46:51 | Ornella Carrano | SI |
| 1/3/24 11:46:54 | Alessia Pironaci | SI |
| 1/3/24 11:47:03 | Assunta Damiano | SI |
| 1/3/24 11:47:08 | Salvatore Tulumello | SI |
| 1/3/24 11:47:09 | Sergio Fey | SI |
| 1/3/24 11:47:15 | Pierpaolo Pisano | SI |
| 1/3/24 11:47:16 | Andrea Arcuri | SI |
| 1/3/24 11:47:25 | Mauro Affanni | SI |
| 1/3/24 11:47:27 | Eva Grande | SI |
| 1/3/24 11:47:29 | Daniela Annunziata | SI |
| 1/3/24 11:47:41 | Roberta Muraca | SI |
| 1/3/24 11:48:25 | Tiziana Esposito | SI |
| 1/3/24 11:50:02 | Maria Visone | SI |
| Sottoscrizione verbale | Giuseppe Raineri | SI |