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

Addì 19 luglio 2023, in Roma
tra

TIM S.p.A.

e

le Organizzazioni Sindacali SLC-CGIL, FISTel-CISL, UILCom-UIL, UGL Telecomunicazioni, unitamente al Coordinamento Nazionali delle RSU

Premesso che

- nell'ambito del *Programma di Digital Enterprise Transformation*, TIM si è dotata di un sistema di soluzioni per la gestione automatizzata della governance dei controlli;
- in tale contesto, le funzioni di Sicurezza e Controllo Interno (ad esempio Audit e Compliance), con l'obiettivo di abilitare logiche di *control monitoring*, hanno manifestato la necessità di adottare strumenti evoluti a supporto delle proprie attività di controllo, anche al fine di ottemperare a quanto previsto dal d.lgs. n. 231/2001 con riferimento alla rilevazione di possibili condotte illecite all'interno dell'organizzazione aziendale;
- pertanto, si rende necessaria l'adozione di sistemi che assicurino il rispetto della compliance aziendale alla normativa in materia di anticorruzione e di informativa economico-finanziaria a prevenzione della commissione di eventuali illeciti (ad es. false comunicazioni sociali) e/o possibili anomalie dei processi aziendali (es. errori anche di tipo materiale derivanti da errata computazione/digitazione voci di contabilità/bilancio);
- 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 esclusivamente per le esigenze indicate al comma 1 dell'art.4, Legge n.300/70, previo accordo sindacale;

- con il presente accordo le Parti, nel rispetto di quanto previsto dal sopra citato art. 4 della legge n. 300/1970, intendono regolamentare l'introduzione e l'utilizzo da parte delle Funzioni di sicurezza e controllo interno di TIM delle piattaforme informatiche finalizzate a rilevare possibili anomalie dei processi aziendali inclusi nel perimetro di

monitoraggio delle Funzioni stesse e/o transazioni potenzialmente strumentali alla realizzazione di comportamenti illeciti;

- in particolare, tali piattaforme (Sap Bis e Celonis) operano attraverso l'analisi di file/flussi dati generati da sistemi informativi aziendali al fine di consentire, da un lato, la ricostruzione su base automatizzata – come più oltre descritto - dell'architettura di funzionamento dei processi aziendali associati e il miglioramento dell'operatività degli stessi (c.d. attività di Process Mining ed Execution Management), dall'altro, la rilevazione, tramite l'attivazione di indicatori di anomalia, di transazioni che potrebbero sottendere situazioni a rischio di comportamento illecito;

- TIM ha illustrato alle Organizzazioni Sindacali le suddette finalità che giustificano l'adozione di detti strumenti, confermando l'intenzione di non utilizzare gli applicativi informatici per il controllo dell'attività lavorativa svolta dai singoli dipendenti.

Tutto ciò premesso, si conviene quanto segue.

1. Adozione ed implementazione dei sistemi di Rilevamento e Gestione Anomalie (di seguito i "Sistemi")

1.1. I sistemi effettueranno, per le esigenze indicate al comma 1 dell'art. 4, legge n. 300/1970, la rilevazione in modo automatico delle informazioni relative a operazioni anomale o che facciano ipotizzare la commissione di illeciti (anche con riferimento ai reati ricadenti nel perimetro del d.lgs. n. 231/2001), permettendo l'accesso solo a dati pseudonimizzati.

Ciascun sistema effettuerà, per gli ambiti di competenza, analisi sulle transazioni concluse nei sistemi autorizzati nei differenti processi di business presidiati riferite, a titolo esemplificativo, a:

- gestione delle offerte commerciali (*retail/wholesales*) e relativi processi di assistenza, vendita, amministrativi e di fatturazione;
- gestione dei processi di *assurance* e *delivery* dei servizi ai clienti;
- gestione dei processi di investimento, degli approvvigionamenti di beni e di servizi e dei relativi processi amministrativi e finanziari;
- gestione dei magazzini e dei relativi processi di logistica;
- gestione dei fornitori e dei *business partner*;
- gestione dei processi di incentivazione;
- rendicontazione costi e approvazione delle spese.

1.2. I sistemi tratteranno le transazioni eseguite dal dipendente nel corso delle attività indicate al precedente paragrafo 1.1 In una prima fase, l'analisi delle transazioni concluse sarà effettuata in modalità automatica senza procedere a identificazione del soggetto cui è riferita l'esecuzione della transazione. In particolare, tale verifica consiste nella lettura automatica da parte dei sistemi informatici dei file di log (accesso, attività) e/o dei flussi dati generati dagli applicativi in uso da parte dei dipendenti. In questa fase non saranno intellegibili i dati identificativi dei singoli dipendenti e l'analisi sarà svolta solo su dati aggregati, statistici o pseudonomizzati.

L'analisi sarà finalizzata all'individuazione di eventi anomali/non conformi e/o rilevatori di possibili condotte illecite.

1.3. Eventuali successivi approfondimenti delle transazioni (quali ad esempio, l'analisi sulla ripetitività dell'evento anomalo/non conforme, l'individuazione di accessi e attività non autorizzati o di un possibile schema di corruzione) si svolgeranno, in modalità manuale, ricorrendo al personale delle funzioni di Sicurezza e Controllo interno e/o del *control owner*, evitando l'adozione di controlli massivi e indiscriminati su dati non pseudonimizzati.

1.4. Solo nel caso in cui l'esito dei predetti approfondimenti confermasse la possibile esistenza di un comportamento illecito o disciplinarmente rilevante ai sensi del sistema sanzionatorio previsto nel modello di organizzazione, gestione e controllo di TIM, le funzioni di sicurezza e controllo interno segnaleranno l'evento alla funzione addetta all'Anti-Frode che si attiverà per:

- rendere intellegibili le informazioni concernenti l'evento anomalo/non conforme, ivi compresa la matricola o il nominativo del dipendente cui tale operazione è riconducibile;
- svolgere le necessarie attività di intelligence/investigation;
- coinvolgere, se necessario, le ulteriori competenti funzioni.

2. Categorie dei dati trattati e finalità

2.1. I dati di cui al paragrafo 1.2 saranno trattati esclusivamente per finalità previste dall'art. 4 co.1, Legge n. 300/1970, in stretto raccordo e nel rispetto delle discipline previste dal Regolamento (UE) 2016/679 sulla privacy (General Data Protection Regulation) e dal D.Lgs. n. 196/2003 (il Codice Privacy) così come modificato dal D.Lgs. n. 101/2018.

2.2 I dati individuali non potranno essere utilizzati per verificare il corretto adempimento, qualitativo e quantitativo, 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, per i quali l'Azienda potrà procedere in parallelo a segnalare/denunciare i fatti all'Autorità Giudiziaria.

3. Conservazione

3.1 In stretta osservanza dell'articolo 5 del GDPR comma "e" (limitazione della conservazione) ed "f" (integrità, riservatezza), i dati sottoposti alle analisi effettuate in modalità automatica saranno conservati esclusivamente da soggetti/strumenti autorizzati per massimo 13 mesi dalla loro generazione più il tempo tecnico per la loro cancellazione comunque non superiore ad un mese, mentre le copie dei dati o dei file memorizzati sulle postazioni di lavoro, se oggetto di analisi da cui si rendesse necessaria una successiva e conseguente segnalazione di sicurezza, saranno

conservate da 24 ore fino a 90 giorni, in funzione della tipologia di segnalazione di sicurezza e della profondità della analisi svolta.

3.2 Nel caso in cui l'esito delle verifiche confermi l'ipotesi dell'esistenza di un comportamento illecito, in linea con le previsioni dell'art. 5 del GDPR che recita "i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati", i dati potranno essere conservati per un tempo maggiore di 13 mesi, e comunque congruo, solo fino all'espletamento della gestione della segnalazione e fino alla definizione di eventuali procedimenti giudiziari, qualora sopraggiunti nel predetto periodo di conservazione (max 14 mesi).

3.3. L'Azienda garantisce che, in coerenza con le modalità indicate dal Garante per la Protezione dei Dati Personali, saranno previsti diversi livelli di accesso ai sistemi, secondo quanto di seguito indicato, avendo riguardo anche ad eventuali interventi per esigenze di manutenzione.

4. Soggetti legittimati all'accesso dei dati

4.1. L'accesso ai dati raccolti e conservati è previsto solo per le finalità indicate al punto 2.1 ed è consentito esclusivamente alle funzioni aziendali preposte alle attività di Controllo Interno e di Sicurezza per lo svolgimento delle competenti attività di verifica tecnica, in coerenza con il presente accordo e le policy aziendali.

5. Informativa

5.1. In coerenza con la normativa vigente, sarà data ai lavoratori interessati adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, e del rispetto dei principi stabiliti dal Regolamento UE 2016/1970 (*General Data Protection Regulation*) in materia di protezione dei dati personali.

6. Verifiche

6.1. Le Parti si danno atto che si incontreranno, su richiesta di una o, comunque, entro sei mesi dalla data del presente accordo al fine di monitorare l'andamento del processo. Altresì, in caso di evidenza di eventuali criticità legate all'applicazione del presente accordo, le Parti (ivi compresa la RSU dell'unità produttiva di riferimento) si incontreranno a richiesta.

6.2. Le Parti concordano che le eventuali evoluzioni tecnologiche e digitali dei sistemi saranno implementate nel rispetto di quanto convenuto nel presente accordo, dandone relativa informativa.

6.3. Le Parti si danno atto che, in caso di apprezzabili innovazioni, modifiche o integrazioni legislative, si incontreranno per verificare la coerenza del presente accordo col mutato quadro legislativo di riferimento.

6.4 Le Parti si impegnano a definire specifiche intese volte a recepire i contenuti del presente accordo nelle Società del Gruppo che applicano il CCNL TLC.

Letto, confermato e sottoscritto in via telematica.

per TIM S.p.A.

per SLC-CGIL

per FISTel-CISL

per UILCOM-UIL

per UGL Telecomunicazioni

per Coordinamento RSU