Verbale di Accordo

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

Roma, 28 maggio 2021

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

A. con il presente accordo le Parti intendono disciplinare le attività di verifica eseguite dalle funzioni *Servizi per l'Autorità Giudiziaria* (SAG) e *Fraud Management*, in ambito *Security*, sulle attività svolte dal personale appartenente alle medesime funzioni (cd. controlli di primo livello), per il tramite degli strumenti adottati a tal fine;
B. il presente accordo osserva le disposizioni del Regolamento UE 2016/679 che, tra l'altro, all'art. 24 sancisce il principio di accountability e di responsabilizzazione per il Titolare del trattamento, e dell'art. 32 che impone l'adozione di adeguate misure di sicurezza da implementare, anche a garanzia degli strumenti elettronici;
C. l'attività di servizi per l'autorità giudiziaria di TIM, per assicurare l'erogazione delle prestazioni obbligatorie di giustizia richieste dall'Autorità Giudiziaria ai sensi dell'art. 96 del Codice delle Comunicazioni Elettroniche (D.Lgs. 259/03), utilizza sistemi IT dedicati (di seguito Sistemi Autorità Giudiziaria) a cui ha accesso il personale addetto all'attività, in ottemperanza ai requisiti previsti dalle normative vigenti e dalle policy aziendali;
D. la vigente normativa per la Protezione dei Dati Personali richiede, ai fornitori di servizi di comunicazione elettronica che svolgono le attività su richiesta dell'Autorità Giudiziaria, di adottare modalità di trattamento dei dati e di sviluppo di strumenti informatici idonei ad assicurare nel pieno rispetto delle leggi in materia, la verifica delle attività svolte da ciascuna persona autorizzata al trattamento dei dati personali;
E. per garantire il principio della *Segregation of Duties*, sancito nel Provvedimento del Garante Privacy del 17/01/2008 nonché indicato nelle policy aziendali, ovvero, creare una netta separazione dei ruoli che eviti conflitti di interessi ed eventuali frodi, impedendo che la stessa persona svolga più parti dello stesso processo, per

cui il personale delegato alle verifiche è distinto rispetto al personale operativo che esegue i trattamenti durante la lavorazione delle prestazioni;

F. è in fase di adozione una piattaforma di Fraud Management System di contrasto e di intelligence sui comportamenti fraudolenti della clientela retail sui servizi fissi e mobili, nonché di analisi investigative per l'individuazione di fenomeni complessi di frodi;
G. è necessario prevedere una verifica delle attività di contrasto e prevenzione frodi con l'obiettivo di evitare trattamenti illeciti dei dati della clientela da parte del personale;
H. 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. 300/1970, previo accordo sindacale.

Tutto ciò premesso si conviene quanto segue:

1. Oggetto dell'accordo

Il presente accordo ha ad oggetto la regolamentazione (ex art. 4 co. 1 Statuto dei Lavoratori) delle piattaforme informatiche utilizzate:

- per le attività di servizi per l'autorità giudiziaria di TIM (attività di gestione delle prestazioni obbligatorie di giustizia, richieste dall'Autorità Giudiziaria e/o soggetti autorizzati - es. richieste di Studi Legali effettuate per finalità difensive degli assistiti - ed espletate dal personale che utilizza la piattaforma Sistemi Autorità Giudiziaria, SAG);
- per le attività di contrasto e prevenzione frodi nei confronti del personale che utilizza la piattaforma di Fraud Management System.

1.1 Sistemi Autorità Giudiziaria

1.1.1 L'obiettivo delle verifiche è quello di assicurare la legittimità delle attività svolte rispetto alle richieste pervenute, in conformità con la normativa vigente.

1.1.2 Le verifiche sono effettuate sulle attività di gestione delle prestazioni svolte dal personale addetto all'attività secondo i criteri di legittimità di seguito riportati:

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

• visualizzazione del dato identificativo del personale che ha gestito la singola prestazione (nominativo o «matricola») solo laddove necessario (come specificato al punto 1.1.4);

• rispetto dei principi applicabili al trattamento dei dati personali in conformità all'art. 5 del Regolamento UE 2016/679: liceità, correttezza, trasparenza, limitazioni delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

1.1.3 Le verifiche sono effettuate dal delegato della funzione (la cui nomina è comunicata al Responsabile della funzione) sulla base della reportistica estratta automaticamente, periodicamente dai Sistemi Autorità Giudiziaria, oppure, sulla base dei report richiesti alle funzioni tecniche competenti per verifiche a campione o al 100%.

1.1.4 Il delegato della funzione analizza la reportistica di cui al punto 1.1.3 e, laddove rilevi non conformità con la normativa vigente nonché con le procedure aziendali, gestisce le azioni correttive. In particolare:

- coinvolge il Responsabile o coordinatore di riferimento comunicando le non conformità riscontrate, in modo da indirizzare le azioni correttive al proprio interno;
- provvede alla correzione della non conformità utilizzando le funzionalità disponibili sui Sistemi Autorità Giudiziaria.

L'esito delle verifiche è rappresentato all'interno dei report di sintesi, predisposti periodicamente in forma anonima.

1.1.5 Solo nel caso in cui l'esito dei predetti approfondimenti confermi l'ipotesi dell'esistenza di un comportamento illecito, l'attività di servizi per l'autorità giudiziaria di TIM preposta alle verifiche, segnalerà al Responsabile o coordinatore le informazioni rese intellegibili concernenti la non conformità, ivi compresa la matricola o il nominativo cui tale operazione è riconducibile, al fine di consolidare l'esito delle azioni a tutela aziendale e del lavoratore ed adottare le opportune iniziative di coinvolgimento delle funzioni competenti.

1.2 Fraud Management System

1.2.1 Le verifiche saranno effettuate sugli accessi e sulle attività del personale della funzione Fraud Management eseguiti tramite la piattaforma secondo i criteri di legittimità di seguito riportati:

- verifiche ex-post e non in tempo reale (rilevazione delle informazioni su attività non modificabili, non effettuate in *real time* o *near real time*);
- visualizzazione del dato nominativo o «matricola» solo nel caso in cui si rilevino attività non correlate ad esigenze di lavoro (come specificato al punto 1.2.4);
- rispetto dei principi applicabili al trattamento dei dati personali in conformità all'art. 5 del Regolamento UE 2016/679: liceità, correttezza, trasparenza, limitazioni delle

finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

1.2.2 In una prima fase l'analisi sarà effettuata in modalità automatica. Tale verifica consiste nell'estrazione periodica a cura degli Amministratori di Sistema dei log di accesso ai dati contenuti nella piattaforma e nella riconciliazione dei dati estratti attraverso l'associazione automatica del log alla lavorazione di una pratica presente nei sistemi. Nell'estrazione non è identificato l'autore dell'accesso ai dati.

Gli Amministratori di Sistema sono appositamente designati 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".

1.2.3 In una seconda fase, solo per i casi non riconciliati automaticamente nella fase precedente, saranno effettuati, in modalità manuale, da parte dei Responsabili della funzione che gestiscono le attività di contrasto e prevenzione frodi e loro Delegati, individuati tra coloro i quali non svolgono le funzioni oggetto di verifica (SOD), ulteriori approfondimenti (quali ad esempio, l'analisi sulla ripetitività dell'evento, l'individuazione di accessi e attività non autorizzati). Si opera in questa fase con dati non identificabili evitando, in questo modo, l'adozione di verifiche massive e indiscriminate su dati in chiaro.

1.2.4 Solo nel caso in cui l'esito dei predetti approfondimenti confermi l'ipotesi dell'esistenza di un comportamento illecito, la funzione che gestisce le attività di contrasto e prevenzione frodi chiederà agli Amministratori di Sistema di rendere intellegibili le informazioni concernenti la non conformità, ivi compresa la matricola o il nominativo cui tale operazione è riconducibile, al fine di consolidare l'esito delle azioni a tutela aziendale e del lavoratore ed adottare le opportune iniziative di coinvolgimento delle funzioni competenti.

2. Categorie dei dati trattati e finalità

2.1 I dati saranno trattati esclusivamente per finalità previste dall'art. 4 co. 1 Statuto dei Lavoratori.

2.2 I dati trattati sono le attività e gli accessi effettuati sui Sistemi Autorità Giudiziaria e Fraud Management System ed i dati identificativi dell'operatore che ha gestito la richiesta.

2.3 I dati relativi al tracciamento delle attività e degli accessi rispettivamente sui Sistemi Autorità Giudiziaria e Fraud Management System possono essere utilizzati, oltre che dalle funzioni tecniche in ambito *Security*, da quelle preposte alle attività di verifica di audit e di compliance per lo svolgimento delle competenti attività, in coerenza con le policy aziendali.

2.4 I dati individuali 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.

3. Conservazione

3.1 I dati (Log) relativi agli accessi e alle attività, saranno conservati per 12 mesi dalla loro generazione, unitamente alle evidenze delle verifiche (Report).

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 12 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 (12 mesi).

4. Informativa

In coerenza con la normativa vigente, sarà data ai lavoratori adeguata informazione delle modalità d'uso degli strumenti (art. 4 Legge n.300/1970) e di effettuazione delle verifiche, e del rispetto dei principi stabiliti dal Regolamento UE 2016/679 (General Data Protection Regulation) in materia di protezione dei dati personali.

5. Verifiche

5.1 Le Parti si danno atto che si incontreranno, a richiesta di una delle Parti e comunque entro sei mesi dalla data del presente Accordo, per monitorare l'andamento del processo.

5.2 Le Parti concordano che le modifiche ai Sistemi Autorità Giudiziaria e Fraud Management System derivanti dall'evoluzione tecnologica digitale, qualora comportino una modifica rispetto a uno dei paragrafi 2,3,4 dell'accordo, saranno oggetto di informativa e verifica tra le Parti firmatarie del presente accordo.

per TIM S.p.A.

per SLC-CGIL

per FISTel-CISL

per UILCOM-UIL

per UGL Telecomunicazioni

per Coordinamento RSU

Accordo 28 maggio 2021

SEGRETERIE NAZIONALI	FAVOREVOLE	CONTRARIO
SLC-CGIL	X	
FISTel-CISL	X	
UILCom-UIL	X	
UGL Telecomunicazioni	X	