Verbale di Accordo sull'uso di sistemi informatici

ai sensi dell'art.4, comma 1 della Legge n.300/70

Roma, 25 febbraio 2021

tra

TIM S.p.A.

e

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

Premesso che

- L'AGCOM, dopo aver effettuato una dettagliata attività di vigilanza, ha pubblicato il 2 ottobre 2018 la delibera 396/18/CONS, in cui ha elencato una serie di attività che TIM e gli altri Operatori devono mettere in campo allo scopo di impedire eventuali usi impropri dei dati wholesale di Assurance;
- al fine di ottemperare alle disposizioni della Delibera AGCOM 396/18/CONS, TIM ha realizzato un sistema (denominato SecOLO) che opera una criptazione dei dati personali dei clienti OLO, nel momento in cui sono acquisiti nei sistemi TIM, sostituendo tali dati con un identificatore unico detto token e memorizzandoli su un nuovo data base protetto ed esterno ai sistemi di Assurance;
- in riferimento all'introduzione di tale sistema l'Azienda si è impegnata a svolgere un'attività di sensibilizzazione e formazione di tutti i lavoratori interessati sull'utilizzo del suddetto sistema e delle credenziali personali d'accesso in modo coerente con quanto previsto dalle disposizioni dell'AGCOM;
- in data 6 novembre 2019, le Parti hanno sottoscritto un'intesa ai sensi dell'art.4, comma 1 della Legge n.300/70 che ha definito le modalità di implementazione del sistema SecOLO, nonché di utilizzo e conservazione dei dati da esso rilevati, riferiti agli accessi/visualizzazioni di anagrafica e recapito telefonico del cliente (data, ora e identificativo di chi accede) effettuati dal personale tramite i seguenti sistemi: Barra Telefonica, e-Star, TTMWEB-OLO, TTM-ARS, nWFM;
- in azienda sono presenti altri sistemi informatici che contengono i dati dei clienti retail e wholesale (eventualmente presenti anche nei campi note) e che consentono agli operatori di accedere ai dati dei clienti, necessari per svolgere la prestazione lavorativa;

- a tutela dell'Azienda e dei lavoratori stessi, al fine di registrare gli accessi non autorizzati e/o ingiustificati ai dati dei clienti, le Parti intendono ampliare la tipologia dei dati protetti ed estendere il sistema SecOLO anche ai restanti sistemi informatici di cui al punto precedente.

Tutto ciò premesso si conviene quanto segue

1. Adozione ed implementazione del sistema SecOLO

1.1. TIM, in analogia alle misure adottate in ottemperanza alle disposizioni contenute nella delibera AGCOM 396/18/CONS a protezione dei dati wholesale di Assurance rilevati attraverso Barra Telefonica, e-Star, TTMWEB-OLO, TTM-ARS, nWFM estenderà a tutti i sistemi informatici aziendali, che contengono i dati dei clienti retail e wholesale (eventualmente presenti anche nei campi note) il sistema SecOLO che registrerà tutti gli accessi/visualizzazioni di anagrafica e recapito telefonico del cliente (data, ora, identificativo di chi accede, dati del cliente visualizzati) effettuati dal personale.

1.2. In caso di necessità di accesso a tali dati, protetti dal meccanismo di tokenizzazione, il personale autorizzato su base profilo (sulla base del principio del need-to-know) potrà detokenizzare i codici alfanumerici per ricondurre in chiaro i dati del cliente.

2. Soggetti legittimati all'accesso dei dati

2.1 I soggetti autorizzati ad accedere al tracciamento degli accessi/visualizzazioni effettuati ai dati dei clienti e al trattamento dei relativi dati sono gli amministratori di sistema 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", il personale della funzione Audit e il personale in ambito Security preposto alla gestione degli incidenti di sicurezza, alla prevenzione delle frodi interne ed esterne.

2.2 Tali soggetti autorizzati 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. Finalità e trattamento dei dati

3.1. In considerazione dell'applicazione/estensione del sistema SecOLO ai sistemi informatici che contengono i dati dei clienti retail e wholesale, i dati raccolti saranno trattati secondo la disciplina dettata dal d.lgs 196/2003 novellato dal d.lgs 101/18 e Regolamento 2016/679/UE in materia di protezione dei dati personali, nonché secondo la disciplina lavoristica in materia di impiego di "strumenti dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori" ex articolo 4, della legge n 300/1970 come modificato dall'articolo 23 del decreto legislativo numero 151/2015.

3.2. In presenza di procedimenti avviati dall'Autorità per le Garanzie nelle Comunicazioni o da altra Autorità Amministrativa circa possibili utilizzi illeciti dei riferimenti dei clienti, i dati acquisiti dagli amministratori di sistema verranno da questi comunicati alla stessa in forma univoca ma non nominativa, nel pieno rispetto del principio di minimizzazione dei dati.

3.3. I dati idonei ad identificare i soggetti che hanno concretamente effettuato l'accesso verranno forniti dai soggetti di cui al punto 2, all'Autorità Giudiziaria o alla Polizia Giudiziaria nell'ambito di procedimenti di indagine ovvero giudiziari.

3.4. 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 denunciati all'Autorità Giudiziaria / Polizia Giudiziaria ovvero pervenissero a TIM verbali di accertamento e contestazione di AGCOM o di altra Autorità Amministrativa conseguenti a segnalazioni di utilizzo improprio di informazioni aziendali riferite a specifiche utenze / clienti.

4. Conservazione dei log di accesso/visualizzazione

4.1 Il tempo previsto per la conservazione dei tracciamenti è di 12 mesi al fine di individuare fenomeni ricorrenti e sviluppare controlli almeno annuali; nel caso in cui non si evidenzi l'esistenza di una possibile frode o incidente di sicurezza di natura rilevante i dati saranno cancellati al superamento del periodo di conservazione previsto.

4.2 Nel caso in cui i dati evidenzino l'esistenza di una possibile frode o incidente di sicurezza di natura rilevante o in presenza di attività di indagine, procedimenti amministrativi o giudiziari, gli stessi saranno conservati per il tempo necessario alla conclusione delle azioni avviate a tutela della società e dell'eventuale relativo iter giudiziario o amministrativo.

5. Informativa

5.1 In coerenza con la normativa vigente sarà data ai lavoratori adeguata e puntuale informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli nel rispetto dei principi stabiliti dalla normativa sulla protezione dei dati personali, in particolare con riferimento al Regolamento UE 2016/679 (General Data Protection Regulation).

6. Disposizioni finali

6.1 Le Parti si danno atto che si incontreranno entro sei mesi dall'avvio operativo del sistema per monitorare l'andamento del processo.

6.2 Le Parti concordano che le eventuali evoluzioni del sistema derivanti dallo sviluppo tecnologico e digitale saranno implementate nel rispetto di quanto convenuto nel presente accordo.

6.3. Le Parti concordano che il presente accordo supera la precedente intesa per l'introduzione del sistema SecOLO stipulata il 6 novembre 2019.

TIM S.p.A.

SLC CGIL

FISTEL CISL

UILCOM UIL

UGL Telecomunicazioni

Coordinamento RSU TIM

Accordo SecOLO – 25 febbraio 2021

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