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

Roma, 14 dicembre 2022

tra

TIM S.p.A.
anche in rappresentanza delle Società del Gruppo che applicano il CCNL TLC

e

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

Premesso che

- a tutela del patrimonio aziendale l'Azienda intende adottare un sistema di Sicurezza Informatica (d'ora in avanti "cybersecurity") che risulti adeguato a fronteggiare i nuovi attacchi informatici (d'ora in avanti "attacchi") che possono derivare anche dall'introduzione di nuove tecnologie, come il 5G o dall'erogazione di nuovi servizi (es. DAZN) o dall'adozione del Cloud, implicando una variazione del contesto di riferimento e l'insorgenza di nuove minacce ad esso correlate;
- la cybersecurity ha l'obiettivo di proteggere i sistemi, le reti e i programmi dagli attacchi digitali. Questi attacchi informatici sono solitamente finalizzati all'accesso, alla trasformazione o alla distruzione di informazioni sensibili, nonché all'estorsione di denaro agli utenti o all'interruzione dei normali processi aziendali;
- gli attacchi possono essere suddivisi in tre categorie:
  1. Cybercrimine: commessi da attori singoli o gruppi che attaccano i sistemi per ottenere un ritorno economico o provocare interruzioni nelle attività aziendali
  2. Cyberattacchi: spesso aventi lo scopo di raccogliere informazioni per finalità illegittime/illecite
  3. Cyberterrorismo: punta a minare la sicurezza dei sistemi elettronici per suscitare panico o paura
- gli attacchi all'interno ed all'esterno dell'azienda possono provenire da tre categorie di soggetti: l'utente interno, l'appaltatore o le terze parti tramite accesso esterno/interno, il malintenzionato o ladro di credenziali di accesso;
- la frequenza degli attacchi informatici esterni ed interni e il loro costo medio sono drasticamente aumentati negli ultimi due anni a livello mondiale, le indagini post attacco sono il centro di costo in più rapida crescita;
- il rischio di attacchi cyber è considerato fra quelli ad alto impatto ed elevata probabilità di accadimento, al quarto posto fra i "clear and present dangers" dopo pandemie, crisi umanitarie, disastri climatici;
- nel rispetto delle leggi, delle policy della privacy delle lavoratrici e dei lavoratori e delle linee guida di Security adottate nel Gruppo TIM, l'Azienda conferma la strategicità delle

stesse in una dinamica che permetta, consolidi e rafforzi la leadership del gruppo TIM nel mercato di riferimento, anche attraverso accordi sindacali il cui fine è il miglioramento della sicurezza aziendale in termini di analisi del rischio nella sicurezza del trattamento dei dati, di riservatezza salvaguardando la privacy dei dati aziendali e delle lavoratrici e dei lavoratori attraverso la crittografia come misura di sicurezza normata dal GDPR all'articolo 32[1] – Sicurezza del trattamento - ed attraverso la pseudonimizzazione e la cifratura dei dati personali, ove tecnicamente implementabili, ovvero disponibili sul mercato, tali da rendere i suddetti dati incomprensibili a chiunque non sia autorizzato ad accedervi utilizzando ad esempio la full disk encryption implementabile su ogni computer a partire dai computer portatili più soggetti a furto o smarrimento, restringendone così l'accesso, garantendo l'integrità, l'accuratezza, l'affidabilità delle informazioni e la disponibilità, assicurandone l'accesso ai soli utenti autorizzati;

- 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;
- in questo contesto, grande valore hanno le relazioni industriali, realizzate attraverso il confronto tra le parti ed i relativi accordi sindacali.

Tutto ciò premesso si conviene quanto segue

1. Oggetto dell'accordo: implementazione del sistema di Cybersecurity

1.1. Allo scopo di tutelare il patrimonio aziendale, i lavoratori/le lavoratrici e i clienti da tutte le tipologie di attacchi informatici nella rete, e da utilizzi erronei dei dispositivi in uso, dei sistemi, al fine, quindi, di limitare/ridurre i rischi, TIM intende dotare la piattaforma di Cybersecurity dei seguenti sistemi:

a) **sistemi di protezione delle comunicazioni** (per comunicazione si intende il flusso dinamico dei dati sulla rete, d'ora in avanti "comunicazione"), in grado di analizzare le comunicazioni, al fine di bloccare i software o i comandi malevoli presenti, di acquisire copia dei contenuti pericolosi, di rilevare, identificare e bloccare i dati aziendali inviati verso siti non autorizzati, di inibire accessi ad indirizzi IP esterni considerati non sicuri, di rilevare e bloccare gli accessi anomali alle reti aziendali, di generare segnalazioni automatiche per gli incidenti di sicurezza rilevati (cfr. 4.1);

b) **sistemi di protezione degli accessi,** per assicurare l'accesso sicuro ai sistemi aziendali solo previa identificazione degli utenti, di autenticare le credenziali di

[1] **Articolo 32 - Sicurezza del trattamento**
1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

accesso, di rilevare e bloccare gli accessi non autorizzati, di abilitare la visibilità ai dati in base ai profili degli utenti;

c) **sistemi di protezione dei dispositivi mobili e delle postazioni di lavoro,** per proteggere i dati su di essi conservati, in grado di abilitare e proteggere l'accesso ai dati aziendali, per analizzare i file memorizzati e le operazioni su di essi effettuate dai dipendenti e dal personale esclusivamente autorizzato al trattamento dei dati (ad es. l'analisi svolta dall'antivirus sul singolo file), di rilevare e bloccare gli eventi significativi ai fini della sicurezza, di acquisire copia dei file compromessi, previa segnalazione al lavoratore (cfr. 4.1);

d) **sistemi di analisi degli eventi di sicurezza,** per individuare eventi significativi che accadono all'interno della rete e sui vari sistemi dell'asset informatico aziendale, ai fini delle attività di gestione, controllo della sicurezza, contenimento dei rischi ad essa correlati e protezione dei dati conservati nei sistemi aziendali.

1.2. Le verifiche sono basate sull'analisi massiva e automatica degli eventi: solo in presenza di *alert* che indicheranno l'effettiva presenza di anomalie (ad es. a seguito di 100 accessi consecutivi con password errata con uno stesso account, oppure presenza di un virus segnalato da Istituzione/Ente Pubblico) rispetto ai modelli statisticamente previsti a riguardo di possibili rischi per la sicurezza si potranno svolgere approfondimenti a cura del personale della funzione Security in qualità di persone autorizzate al trattamento dei dati ai fini del GDPR con lo scopo di confermare, identificare e rimuovere l'origine delle minacce e ripristinare il corretto funzionamento e la sicurezza delle reti, dei sistemi, dei dispositivi.

1.3. Tramite il medesimo sistema di Cyber Security saranno eseguiti anche i controlli c.d. di "1° livello" (effettuati seguendo le procedure previste dal sistema di controlli interno) sul personale addetto all'attività di analisi di sicurezza, al fine di evitare trattamenti illeciti dei dati dei dipendenti raccolti a ulteriore garanzia del sistema di controllo.

2. Categorie dei dati trattati e finalità

2.1. I dati 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 e dal recepimento della direttiva Nis attraverso il D. Lgs. N. 65/2018.

2.2. Saranno sottoposti alle verifiche in forma automatica dal sistema di Cybersecurity i tracciamenti degli accessi e delle attività eseguite sui sistemi aziendali, il traffico dati scambiato sulle reti aziendali e su Internet, nonché gli eventi generati dal sistema stesso, nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679 per i dati che possano identificare una persona fisica.

2.3. I dati individuali non potranno essere utilizzati per verificare il corretto adempimento, qualitativo né 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 procederà in parallelo a segnalare/denunciare i fatti all'Autorità Giudiziaria.

2.4. 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, fatti salvi obblighi di legge.

2.5. I dati idonei ad identificare i soggetti che hanno concretamente effettuato l'accesso verranno forniti dai soggetti di cui al punto 4, in parallelo all'Autorità giudiziaria o alla polizia giudiziaria nell'ambito di procedimenti di indagine ovvero giudiziari.

2.6. Le parti firmatarie del presente accordo potranno richiedere attraverso incontri nazionali e/o territoriali evidenze riportanti la corretta implementazione del citato controllo di I livello.

2.7. Ai fini dei controlli di I livello saranno tracciati gli accessi e le attività eseguite dagli analisti sul sistema di Cyber Security stesso.

3. Conservazione

3.1. In stretta osservanza dell'articolo 5 del GDPR comma "e" (limitazione della conservazione) ed "f" (integrità, riservatezza), i dati generati dal tracciamento degli accessi e delle attività saranno conservati esclusivamente da soggetti/strumenti autorizzati per massimo 12 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 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 (max 13 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 ed è consentito esclusivamente agli analisti ed ai responsabili della funzione in ambito Security, agli amministratori di sistema, alle funzioni aziendali preposte alle attività di Audit e di Compliance 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 adeguata informazione in merito alle modalità d'uso degli strumenti e di effettuazione dei controlli, nonché riguardo al rispetto dei principi stabiliti dal Regolamento UE 2016/679 (General Data Protection Regulation) in materia di protezione dei dati personali.

6. Verifiche

6.1. Le Parti si danno atto che si incontreranno entro sei mesi dalla data del presente Accordo per 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 relative ai Sistemi di Cybersecurity derivanti dall'evoluzione tecnologica e digitale, 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.

per TIM S.p.A.

per SLC-CGIL

per FISTel-CISL

per UILCOM-UIL

per UGL Telecomunicazioni

per Coordinamento RSU

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

Estrazione 14 Dicembre 2022 ore 16:50

Completion time	Name	Vuoi sottoscrivere l'accordo relativo al sistema di Cybersecurity, di cui è stata data lettura durante l'incontro di Coordinamento Nazionale RSU del 14 Dicembre 2022?
12/14/22 16:37:25	Luca Fratantonio	Si
12/14/22 16:37:43	Antonio Ingallinella	Si
12/14/22 16:37:45	Giuseppe Rienzo	Si
12/14/22 16:37:45	Roberto Gasparin	Si
12/14/22 16:37:49	Grazia Petito	Si
12/14/22 16:37:53	Giuseppina Pezzulla	Si
12/14/22 16:37:54	Giuseppe Carbone	Si
12/14/22 16:37:55	Giuliano Cerullo	Si
12/14/22 16:37:58	Francesco Spano'	No
12/14/22 16:38:03	Maurizio Tomiello	Si
12/14/22 16:38:05	Chiara Lepschy	Si
12/14/22 16:38:06	Maria Elena Gotti	Si
12/14/22 16:38:07	Licia Bergamo	Si
12/14/22 16:38:11	Pier Luigi Bosi	Si
12/14/22 16:38:13	Roberto Greco	Si
12/14/22 16:38:15	Iuri Nassi	Si
12/14/22 16:38:21	Lorenzo Martinelli	Si
12/14/22 16:38:23	Emanuele Falucca	Si
12/14/22 16:38:24	Paolo Aveta	Si
12/14/22 16:38:28	Fabio Di Russo	Si
12/14/22 16:38:33	Silvano Del Cotto	Si
12/14/22 16:38:34	Fortunato Nucera	Si
12/14/22 16:38:45	Enrico Viatori	Si
12/14/22 16:38:52	Norma Marighetti	Si
12/14/22 16:38:54	Paola Maria Berola	Si
12/14/22 16:38:54	Claudio Giuliani	Si
12/14/22 16:38:54	Roberto Giannotta	Si
12/14/22 16:39:05	Roberto Cocce'	Si
12/14/22 16:39:12	Maurizio Tola	Si
12/14/22 16:39:30	Francesco Vallone	Si
12/14/22 16:39:45	Rosario Marini	Si
12/14/22 16:40:25	Davide Piras	Si
12/14/22 16:40:25	Vincenzo Bellaspica	Si
12/14/22 16:40:32	William Spinelli	Si
12/14/22 16:40:40	Massimo Bellio	Si
12/14/22 16:40:52	Antonio Russo	Si
12/14/22 16:41:28	Mara Errichelli	Si
12/14/22 16:41:29	Antonio Palumbo	Si
12/14/22 16:41:46	Giovanni Piccardo	Si
12/14/22 16:42:14	Giulia Magrini	Si
12/14/22 16:42:14	Eugenio Maurizio Sartori	Si