VERBALE DI ACCORDO AI SENSI DELL'ART.4 LEGGE N.300/70

Roma, 9 settembre 2025, con collegamento in via telematica ed in presenza:

tra

La Società Open Fiber S.p.A.

e

SLC-CGIL, FISTEL-CISL, UILCOM-UIL, UGL Telecomunicazioni Nazionali e Territoriali, unitamente alla Rappresentanza Aziendale

Premesso che

- A tutela del patrimonio aziendale l'Azienda ha implementato un sistema di Sicurezza Informatica (d'ora in avanti "Cybersecurity") al fine di risultare costantemente idoneo a fronteggiare i nuovi attacchi informatici (d'ora in avanti "attacchi") e l'insorgenza di nuove minacce, anche in osservanza a quanto prescritto dalla normativa nazionale e comunitaria;
- Dal 16 ottobre 2024 è in vigore la nuova normativa Network and Information Security (Direttiva NIS2) di derivazione europea. Il recepimento della direttiva con il decreto legislativo del 4 settembre 2024 n. 138 e sue successive determinazioni e altre normative collegate mira a garantire l'aumento del livello di sicurezza informatica del tessuto produttivo e delle Pubbliche Amministrazioni del Paese, in armonia con gli altri Stati membri dell'Unione Europea;
- Inoltre, in applicazione della normativa relativa al PSNC (Perimetro di Sicurezza Nazionale Cibernetica), istituita con Decreto-Legge 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019 n. 133 e altre normative collegate, è indispensabile garantire la sicurezza delle reti, dei sistemi informativi e dei servizi informatici (cosiddetti "beni ICT"), dal cui funzionamento dipende l'esercizio di funzioni e servizi essenziali dello Stato. Per preservare questa sicurezza, la Legge impone determinati obblighi in capo ad amministrazioni pubbliche, enti, e operatori pubblici e privati con sede nel territorio nazionale, che esercitino funzioni o servizi essenziali dello Stato che dipendono dall'utilizzo di reti, sistemi informativi e servizi informatici il cui malfunzionamento, utilizzo improprio, o interruzione, anche parziale, possa causare un pregiudizio alla sicurezza nazionale;
- La Cybersecurity si riferisce a qualsiasi tecnologia, pratica e politica per prevenire gli attacchi informatici o ridurne l'impatto e ha lo scopo di proteggere i sistemi informatici, le applicazioni, i dispositivi, i dati, le risorse finanziarie e le persone da ransomware e altri malware, truffe di phishing, furti di dati e altre minacce informatiche;
- A livello aziendale, la Cybersecurity è una componente chiave della strategia complessiva di gestione del rischio di un'organizzazione;
- Nel rispetto delle leggi e degli standard internazionali relativi alla privacy e alla sicurezza delle informazioni adottate da Open Fiber S.p.A., l'Azienda conferma la strategicità dei propri asset tangibili ed intangibili in una dinamica che permetta, anche attraverso accordi sindacali:
    - il miglioramento della sicurezza aziendale in termini di analisi dei rischi legati al trattamento dei dati e delle informazioni;
    - garantire la privacy dei dati personali delle lavoratrici e dei lavoratori attraverso anche soluzioni tecnologiche quali la cifratura (come riportato dall'articolo 32 del GDPR – Sicurezza del trattamento) e la pseudonimizzazione, ove tecnicamente implementabili (e.g. sistemi legacy) ovvero disponibili sul mercato, tali da rendere i suddetti dati incomprensibili a chiunque non sia autorizzato ad accedervi;
    - garantire in tutte le fasi del trattamento l'integrità, l'accuratezza, l'affidabilità, la disponibilità, la confidenzialità e il non ripudio delle informazioni, 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 anche indirettamente la possibilità di un controllo a distanza dell'attività dei lavoratori possono essere impiegati

esclusivamente nel rispetto delle disposizioni 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 gestione della Cybersecurity

Allo scopo di tutelare il patrimonio aziendale tangibile ed intangibile, i clienti, gli utenti finali e le lavoratrici/i lavoratori da tutte le tipologie di attacchi informatici e da utilizzi involontariamente pericolosi dei dispositivi in uso, dei sistemi e delle reti, al fine, quindi, di limitare/ridurre i rischi, Open Fiber S.p.A. intendere regolamentare e implementare il proprio il sistema di gestione di Cybersecurity, che consta delle seguenti funzionalità:

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 i contenuti e, in base alla necessità,

- monitorare ed intervenire, sul traffico di Comunicazione (es. Inserendo blocchi o filtri);
- di acquisire gli elementi necessari alla prevenzione, al contrasto e all'analisi di fenomeni inerenti la Cybersicurezza;
- di inibire accessi a risorse (e.g. file, informazioni, apparati come workstation o server, etc.) non sicure;
- di rilevare e intervenire sugli accessi anomali ai e dai beni aziendali, nonché di rilevare e intervenire sulle modifiche anomale afferenti ai medesimi;

b) sistemi di protezione degli accessi, per assicurare l'accesso sicuro ai sistemi aziendali solo previa identificazione degli utenti attraverso credenziali; per rilevare, analizzare e intervenire su accessi non autorizzati e/o potenzialmente malevoli; per abilitare l'accesso a risorse specifiche in base ai profili autorizzativi degli utenti;

c) sistemi di protezione dei dispositivi mobili e delle postazioni di lavoro (end point), per proteggere le risorse su di essi conservate (e.g. l'analisi svolta dall'antivirus sul singolo file); per monitorare, analizzare, rilevare e intervenire sugli eventi significativi ai fini della sicurezza; per intervenire sui dispositivi compromessi, con segnalazione al lavoratore e, se necessario, consentire l'intervento da remoto al personale autorizzato per la mitigazione delle minacce (e.g. per intervenire sui processi malevoli in atto sull'end point)(cfr. 4);

d) sistemi di monitoraggio, analisi e correlazione degli eventi di sicurezza, per monitorare, analizzare e rilevare eventi di sicurezza che riguardano le risorse aziendali (e.g. reti, sistemi, informazioni), anche al fine di prevenire o intervenire su possibili incidenti di sicurezza.

Le segnalazioni generate, le verifiche e le azioni conseguenti possono essere basate su analisi massive, automatiche ed intelligenti degli eventi: esclusivamente in presenza di allarmi generati automaticamente, segnalazioni e/o informazioni circa eventi di sicurezza informatica "alert" che indichino l'effettiva e/o potenziale presenza di anomalie legate a possibili rischi per la sicurezza (e.g. in caso di numerosi tentativi consecutivi di accesso con password errata con lo stesso account) si potranno svolgere approfondimenti a cura del personale delle Funzioni Aziendali preposte alle attività di analisi di sicurezza ad oggi le Funzioni *Security & QHSE* e *Information & Communication Technology* e limitatamente alla sicurezza dell'infrastruttura tecnologica aziendale anche la Funzione *Assurance* (di seguito "Funzioni Aziendali Preposte"), in qualità di persone autorizzate al trattamento dei dati ai fini del GDPR con lo scopo di confermare e identificare l'evento (e.g. incidente di sicurezza informatica) e se necessario intervenire sulle risorse aziendali. Per l'espletamento di tali attività si specifica che possono accedere a tali dati anche soggetti esterni appositamente nominati responsabili del trattamento operanti nel settore della sicurezza

aziendale e/o nel Centro Operativo di prevenzione, gestione e risposta degli incidenti, collocati nel territorio comunitario, nel rispetto delle indicazioni impartite dalle sopracitate funzioni.

Tramite i medesimi sistemi di Cyber Security saranno eseguiti anche controlli sul personale delle Funzioni preposte alle 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**

Tali dati saranno altresì trattati, fermo il rispetto dell'Art.4 Legge N.300/70, 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. Saranno sottoposti a controlli di sicurezza, anche in forma manuale, dai sistemi 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 dall'articolo 5 del Regolamento (UE) 2016/679 per i dati da cui può derivare, anche indirettamente, l'identificazione di una persona fisica. Le attività di trattamento dei dati personali che deriverebbero dall'implementazione dei sistemi riportati al punto 1. "Oggetto dell'accordo" sono legittimate dalle seguenti basi giuridiche:

- adempiere un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, comma 1, lettera c));
- il perseguimento del legittimo interesse del titolare del trattamento (art. 6, comma 1, lettera f)).

I dati personali trattati non potranno essere utilizzati per verificare il corretto adempimento, né qualitativo né quantitativo, della prestazione lavorativa e pertanto non potranno essere diffusi, né utilizzati in altri ambiti aziendali, né trattati ai fini disciplinari e/o valutativi, salvo il caso in cui emergessero evidenze di comportamenti illeciti e/o in casi di dolo o colpa grave per i quali l'Azienda potrà anche procedere in parallelo a segnalare/denunciare i fatti all'Autorità Giudiziaria.

Nel caso di richieste pervenute dalle Autorità competenti che prevedano anche dati personali dei soggetti interessati, tali dati verranno comunicati dai soggetti di cui al punto 4 alle stesse in forma univoca e/o aggregato (in base alla natura della richiesta) ma comunque non nominativa, nel pieno rispetto del principio di minimizzazione dei dati, fatti salvi espliciti obblighi di legge. I dati idonei a identificare i soggetti che hanno concretamente svolto attività illecite (come definite dai paragrafi precedenti) verranno forniti dai soggetti di cui al punto 4, all'Autorità giudiziaria e/o alla polizia giudiziaria nell'ambito di procedimenti di indagine ovvero giudiziari.

Ai fini dello svolgimento dei necessari controlli di sicurezza e di verificare il rispetto delle disposizioni di legge in merito, saranno tracciati gli accessi e le attività eseguite dal personale delle Funzioni Aziendali Preposte alle attività di analisi di sicurezza e dal personale esterno nominato responsabile. Così come disciplinano al punto 4. Soggetti legittimati all'accesso dei dati.

3. Conservazione

In stretta osservanza dell'articolo 5 del GDPR, comma "e" (limitazione della conservazione) e "f" (integrità e riservatezza), i dati generati dal tracciamento degli accessi e delle attività saranno conservati esclusivamente da soggetti e strumenti autorizzati per un periodo massimo di 12 mesi, a partire dalla loro generazione, più il tempo tecnico necessario per la loro cancellazione, che non potrà comunque superare un mese. Tale periodo potrà essere esteso fino a 24 mesi qualora previsto da normative tempo per tempo vigenti ivi compresa la disciplina di cui al Decreto-legge 105/2019 "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*" e ss.mm.ii ed al Decreto Legislativo 134/2024 "*Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio*".

Le copie dei dati o dei file memorizzati sulle postazioni di lavoro, qualora oggetto di analisi che comporti una successiva segnalazione di sicurezza, saranno conservate per un periodo che va da 24 ore a 90 giorni

a partire dalla chiusura dell'evento di sicurezza, in funzione della tipologia di segnalazione di sicurezza e della profondità dell'analisi effettuata.

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 quanto sopraripportato, 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 .

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 a eventuali interventi per esigenze di manutenzione.

4. Soggetti legittimati all'accesso dei dati

L'accesso ai dati raccolti e conservati è previsto solo per usufruire dei servizi offerti dai sistemi riportati al punto 1 "Oggetto dell'accordo" ed è consentito esclusivamente al personale strettamente necessario e formalmente autorizzato. Tali soggetti sono: i) il personale delle Funzioni Aziendali Preposte alle attività di analisi di sicurezza; ii) il personale esterno nominato responsabile.

5. Informativa

In coerenza con la normativa vigente, saranno conferite ai soggetti interessati le informazioni relative al trattamento dei loro dati personali necessari per l'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

Le Parti si danno atto che si incontreranno entro dodici 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 l'eventuale rappresentanza aziendale dell'unità produttiva di riferimento) si incontreranno a richiesta.

Le Parti concordano che le eventuali evoluzioni relative al sistema aziendale di Cybersecurity derivanti dall'evoluzione tecnologica e digitale, saranno implementate nel rispetto di quanto convenuto nel presente accordo dandone relativa informativa.

Le Parti si danno atto che, in caso di apprezzabili innovazioni, modifiche o integrazioni legislative o amministrative (ivi compresi i provvedimenti del Garante per la Protezione dei Dati Personali), si incontreranno per verificare la coerenza del presente accordo col mutato quadro legislativo di riferimento.

Il presente verbale si compone di n.4 pagine.

Letto, confermato e sottoscritto con modalità telematiche ed in presenza da:

Open Fiber S.p.A.

SLC-CGIL FISTEL-CISL UILCOM UIL UGL Telecomunicazioni

Le Rappresentanze Aziendali