ACCORDO SINDACALE

La Direzione Human Capital Officer della Società **CNP Vita Assicura S.p.A.**, qui rappresentata dall'ing. Nicola Sonedda – Chief Human Capital Officer e dalla sig.ra Simona Alessandra Responsabile Administration

e

Le **Rappresentanze Sindacali Aziendali FISAC/CGIL** rappresentate dal Sig. Raffaele Argentiero, **UILCA** rappresentata dal Sig. Sergio Tavian, **SNFIA** rappresentata dal Sig. Antonio Mussari (in seguito, indicate collettivamente come "le Parti")

Premesso che

- nell'ambito del progressivo rafforzamento dei propri presidi di protezione e sicurezza informatica, la Società ha nel tempo adottato sistemi e soluzioni finalizzati alla tutela del patrimonio informativo e degli asset aziendali, oggetto degli accordi sindacali sottoscritti dalle Parti ai sensi dell'art. 4, comma 1, della legge n. 300/1970, tra cui, in particolare, il sistema di *Data Loss Prevention*, *Data Governance* e *Proxy*, successivamente integrato ed esteso, da ultimo, mediante l'adozione della soluzione tecnologica "Netskope Data Loss Prevention" (di seguito, congiuntamente, i "**Precedenti Accordi**");
- La crescente evoluzione delle minacce informatiche richiede l'adozione di misure tecnico-organizzative all'avanguardia per garantire l'integrità del patrimonio aziendale, la continuità dei servizi e la protezione dei dati personali;
- Il presidio di sicurezza denominato Security Operation Center (S.O.C.) è finalizzato all'analisi dei log e alla rilevazione tempestiva di potenziali attacchi o anomalie di sicurezza informatica e si inserisce, quale estensione e integrazione, nel sistema di presidi di sicurezza informatica oggetto dei Precedenti Accordi;
- Le parti firmatarie riconoscono che tali sistemi/presidi, pur operando su infrastrutture e flussi di metadati tecnici relativi agli strumenti di lavoro utilizzati dai dipendenti, non hanno e non devono avere come finalità il controllo a distanza della produttività o della presenza dei lavoratori;
- L'intesa risponde pienamente ai requisiti previsti dall'art. 4, comma 1, della Legge n. 300/1970, per scopi di tutela del patrimonio aziendale e sicurezza dei sistemi;
- L'Azienda garantisce il pieno rispetto del Regolamento UE 2016/679 (GDPR) e delle disposizioni del Garante per la protezione dei dati personali.

Tutto ciò premesso, le Parti convengono quanto segue.

1. Le premesse costituiscono parte integrante del presente accordo.
2. Oggetto e Finalità dell'Accordo:

   L'oggetto del presente accordo è la disciplina delle modalità di funzionamento del sistema S.O.C. Il sistema persegue esclusivamente finalità di sicurezza informatica e protezione del perimetro e patrimonio aziendale. È fatto divieto all'Azienda di utilizzare il S.O.C. e le

informazioni da esso raccolte per monitorare in tempo reale o differito le performance lavorative, i ritmi di produzione, l'attività dei singoli dipendenti e/o per finalità disciplinari fatto salvo quanto previsto dal punto 8 del presente accordo. Le Parti, ai sensi e per gli effetti dell'art. 4, comma 1, della Legge n. 300/1970, convengono sull'utilizzo del S.O.C. per esigenze di tutela del patrimonio aziendale e di sicurezza dei sistemi, nei termini e con le garanzie previsti dal presente accordo.

3. Caratteristiche Tecniche e Funzionamento del S.O.C:

   Il S.O.C. analizza i log e i metadati generati dagli endpoint aziendali (es PC, smartphone), dalla rete (VPN, Firewall), dai server e sistemi, dagli applicativi di produttività aziendale, dai sistemi di sicurezza aziendale e dal Proxy. L'analisi è basata su Indicatori di Compromissione (IoC) o pattern di comportamento anomalo della macchina/rete (es. download massivi, tentativi di accesso da geolocalizzazioni incongruenti, traffico verso indirizzi IP malevoli). Il S.O.C. opera in modalità automatizzata tramite algoritmi di correlazione eventi. L'alerting di sicurezza si attiva unicamente al superamento di precise soglie di anomalia tecnica predefinite.

4. Garanzie dei Dati:
   Il dato tecnico per risalire all'identità specifica di un dipendente sarà utilizzato laddove risulti strettamente indispensabile per investigare e mitigare un incidente informatico. Tale operazione potrà essere effettuata esclusivamente dal personale autorizzato della funzione sicurezza informatica, sotto la responsabilità del CISO, e sarà tracciata. Su richiesta, l'elenco di tali operazioni sarà reso disponibile al Comitato di cui al punto 7, senza indicazione dei lavoratori interessati. L'Azienda garantisce la riservatezza dei dati raccolti, affinché le attività svolte da un/a lavoratore/trice non siano portate a conoscenza di altro personale oltre quello autorizzato.
5. Tempi di Conservazione:
   I log e i metadati raccolti a scopi di sicurezza informatica saranno memorizzati per massimo 12 mesi decorsi i quali verranno cancellati automaticamente, salvo che la conservazione per un periodo ulteriore sia necessaria per la gestione di un incidente di sicurezza in corso, per adempiere a obblighi di legge o a richieste dell'autorità, ovvero per la tutela dei diritti in sede giudiziaria.
6. Informazione ai Lavoratori:
   L'Azienda informerà tutti i lavoratori, ai sensi dell'art. 4, comma 3, della Legge n. 300/1970, con una comunicazione che darà notizia della sottoscrizione del presente accordo e ne illustrerà sinteticamente le finalità, pubblicando sulla Intranet aziendale il presente accordo. La Società aggiornerà inoltre, ove necessario, l'informativa privacy e le policy aziendali.
7. Costituzione del Comitato Paritetico di Controllo e Garanzia:
   Viene istituito un Comitato Paritetico di Controllo e Garanzia, composto in eguale misura da rappresentanti dell'Azienda (incluso il CISO) e le RSA che si riunirà su richiesta motivata di una delle parti al massimo 4 volte all'anno. tutti i membri del Comitato sono tenuti al massimo riserbo verso i terzi su tutte le informazioni ricevute dalla Società per la stipulazione e l'esecuzione del presente Accordo.
   Queste informazioni possono essere utilizzate solo per verificare la corretta applicazione del presente Accordo. Non possono essere copiate, conservate fuori dalle sedi del Comitato né comunicate a terzi, salvo il confronto interno tra i rappresentanti sindacali nei

limiti strettamente necessari. Restano salvi gli obblighi di comunicazione previsti dalla legge e l'esercizio dei diritti davanti all'autorità giudiziaria e alle autorità amministrative competenti. L'obbligo resta in vigore anche dopo la cessazione dell'incarico di rappresentante e dopo la cessazione del presente accordo.

8. Divieto di Utilizzo Disciplinare:
   In conformità con l'art. 4 dello Statuto dei Lavoratori, le evidenze informatiche raccolte, trattate o correlate dal sistema S.O.C. non possono costituire prova o fondamento per l'apertura di procedimenti disciplinari a carico dei lavoratori connessi alla gestione ordinaria dell'attività lavorativa. Resta fermo che eventuali comportamenti fraudolenti, penalmente rilevanti o comunque contrari a norme di legge o alle policy aziendali, saranno gestiti secondo le procedure e le garanzie previste dalla legge e dal contratto collettivo applicabile.
9. Durata dell'Accordo:
   Il presente accordo ha validità a decorrere dalla data di sottoscrizione.

Letto, confermato e sottoscritto.
Milano, 23/10/2026

Per la Società:

CNP Vita Assicura S.p.A.
Chief Human Capital Officer
Nicola Sonedda

CNP Vita Assicura S.p.A.
Head of Administration
Simona Alessandra

Per le OO.SS.:

Antonio Mussari
RSASNFIA

Sergio Tavian
RSA UILCA
