ACCORDO SINDACALE

EX ART. 4 LEGGE N. 300/1970

Il giorno 31 luglio 2026 in modalità telematica,

TRA

il Gruppo Generali (Assicurazioni Generali S.p.A., Generali Italia S.p.A., Genertel S.p.A. Alleanza Assicurazioni S.p.A., Al Futuro S.r.l., GOSP S.r.l., Generali Welion S.c.a.r.l.,), rappresentato dal Dott. Gianluca Perin, dal Dott. Davide Pelucchi e dall'avv. Maria Cristina Muglia

E

i Coordinamenti delle Rappresentanze Sindacali Aziendali FIRST/CISL, FISAC/CGIL, UILCA, FNA e SNIFIA del Gruppo Generali

PREMESSE

a) l'Azienda ha intenzione di adottare un sistema denominato SIEM (Security Information Event Management) allo scopo di rafforzare le misure di sicurezza informatica, rilevare tempestivamente attacchi o anomalie e adempiere a obblighi normativi e di compliance;

b) il sistema raccoglie log (c.d. metadati) provenienti dai seguenti sistemi e applicazioni in uso in azienda:

- Firewall, Web Application Firewall, IDS/IPS, User Proxy, Reverse Proxy;
- Dispositivi di rete (NAC, Switch, Router, ecc.);
- Sistemi di autenticazione di rete (TACACS, RADIUS, ecc.);
- VPN e accessi remoti;
- Identity Management;
- Microsoft 365 (Posta, SharePoint, Teams, ecc.),
- Proxy Netskope cloud;
- Email gateways / Antispam;
- Microsoft Defender for Office (Email Security);
- Antivirus/EDR;
- DNS & DHCP;
- Server infrastructure systems (AD, LDAP, SCCM, ecc.);
- Server OS logs;
- Anti-DDoS solutions;

- Cloud security & audit events;
- Office 365 audit logs;
- Storage;
- RACF;
- Database administration activity;

c) i dati registrati nei log includono:

- indirizzi IP, MAC address, hostname, protocolli e porte di comunicazione, URL richiesti, categorie URL, servizi utilizzati, device di connessione;
- User ID, log di accesso (sign-in/sign-off) e log delle azioni effettuate (audit)
- indirizzi e-mail di mittente e destinatario, oggetto dei messaggi, ID messaggio, presenza e dimensione di eventuali allegati, dimensioni della e-mail, azioni intraprese (deliver, quarantena);
- file/processi sospetti individuati dagli antivirus/EDR, categorizzazione delle attività rilevate;
- timestamp e riferimenti temporali relativi a tutte le azioni registrate;

d) la finalità esclusiva del trattamento dei dati è la sicurezza informatica e, in particolare:

- rilevazione, prevenzione e contrasto di attacchi informatici, accessi non autorizzati, infezioni malware, compromissioni di account;
- gestione di eventi di sicurezza e incident response;
- verifica di conformità a normative e standard internazionali (NIST, ISO/IEC, PCI DSS) e alle linee guida di settore;

Il sistema SIEM tratterà esclusivamente i metadati strettamente indispensabili alla rilevazione, prevenzione e gestione degli eventi di sicurezza informatica, con esclusione dei contenuti delle comunicazioni elettroniche, dei messaggi di posta elettronica, delle chat, dei documenti, degli allegati, delle registrazioni audio/video o di altri contenuti generati dagli utenti e di ogni dato non pertinente o eccedente rispetto a tali finalità.

e) il sistema SIEM è ospitato su infrastruttura cloud in hosting esclusivamente in datacenter Europei – con dati cifrati "*at-rest*" utilizzando sistemi di cifratura industry standards (e.g. AES 256) e "*in-transit*" tramite TLS; l'accesso al sistema è consentito esclusivamente a personale specificatamente autorizzato, tramite autenticazione centralizzata gestita con Azure AD, multi-factor authentication (MFA) e modello di controllo RBAC (Role-Based Access Control);

f) il sistema SIEM non ha e non potrà avere finalità di controllo diretto e/o indiretto sull'attività lavorativa dei dipendenti a fini disciplinari;

g) la conservazione dei log è differente in base alle singole fonti: i log sul SIEM sono conservati per un periodo massimo di 12 mesi, mentre i log nei sistemi di origine hanno periodi di retention differenziati, pari a 90 giorni per i log di accesso

Microsoft 365, 180 giorni per i log di utilizzo (audit) Microsoft 365, 90 giorni per i log di Netskope Proxy e 30 giorni per i log di Microsoft Defender for Office;

h) il trattamento dei dati personali contenuti nel sistema SIEM è effettuato dall'Azienda in qualità di titolare del trattamento (ai sensi del Regolamento UE 2016/679 – GDPR), sulla base giuridica dell'adempimento di un obbligo legale e del legittimo interesse alla sicurezza informatica, nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, integrità e riservatezza, nonche dell'art. 4 della legge 300/1970;

Il presente Accordo è interpretato e applicato in coerenza con i principi del GDPR in materia di metadati, log e strumenti informatici in ambito lavorativo, con particolare riferimento a necessità, proporzionalità, minimizzazione, trasparenza e limitazione della conservazione.

SI CONVIENE E SI STIPULA QUANTO SEGUE

Le premesse costituiscono parte integrante e sostanziale del presente accordo

Art. 1 – Oggetto

Il Gruppo Generali procederà all'installazione e l'utilizzo del sistema SIEM (Security Information and Event Management) , per le finalità, per i modi e nei limiti indicati nelle premesse, destinato alla raccolta, centralizzazione e analisi dei log provenienti dai sistemi e dalle infrastrutture aziendali.

Art. 2 – Finalità

L'utilizzo del sistema SIEM è giustificato e legittimato esclusivamente da esigenze di tutela della sicurezza delle infrastrutture informatiche e dei dati aziendali, e in particolare:

- la rilevazione e la prevenzione di accessi non autorizzati, attacchi informatici, infezioni malware, compromissioni di account e altre minacce cyber;
- la gestione e la risposta ad incidenti di sicurezza (incident response), ivi compresa la ricostruzione degli eventi e l'individuazione delle cause tecniche che hanno reso possibile la violazione;
- l'adempimento a obblighi di legge e a requisiti di compliance in materia di protezione dei dati e sicurezza informatica, nonché il rispetto degli standard e delle best practices riconosciuti a livello internazionale (quali, a titolo esemplificativo, NIST, ISO/IEC, PCI DSS).

Ogni utilizzo del sistema SIEM dovrà essere strettamente limitato a tali finalità, ritenute imprescindibili per garantire la continuità operativa, l'integrità dei sistemi e la protezione del patrimonio informativo aziendale.

Il Gruppo Generali ha effettuato la DPIA - valutazione di impatto e test di bilanciamento ai sensi degli artt. 35 e 6 del GDPR i cui esiti sono stati comunicati alle OO.SS., e procederà all'aggiornamento dell'informativa privacy del personale per fornire una chiara rappresentazione del trattamento dei metadati effettuato ed assicurare la piena trasparenza nei confronti degli interessati. Le Parti confermano l'importanza della

formazione continua a tutto il personale anche sulle tematiche oggetto del presente accordo.

Art. 3 – Esclusione di finalità di controllo dei lavoratori

Le Parti riconoscono espressamente che l'impiego del sistema SIEM non è destinato, né potrà in alcun modo essere utilizzato, per esercitare controlli diretti e/o indiretti sull'attività lavorativa, la prestazione, la produttività, i tempi di lavoro o le modalità di svolgimento dell'attività da parte dei dipendenti nonché la profilazione degli stessi. L'analisi e la conservazione dei log raccolti all'interno del sistema SIEM hanno esclusivamente la funzione di supporto alle attività di sicurezza informatica e resta pertanto esclusa ogni forma di utilizzo che possa contrastare con le garanzie sancite dall'art. 4 dello Statuto dei Lavoratori.

L'eventuale utilizzabilità dei dati raccolti dal SIEM ai fini disciplinari potrà avvenire esclusivamente nei casi previsti dalla legge, quando emergano incidentalmente prove di condotte fraudolente nel rispetto dell'art. 4 della legge 300/1970, del GDPR e delle garanzie procedimentali previste dall'ordinamento

Inoltre i dati e le informazioni raccolti dal sistema non possono essere utilizzati per finalità di valutazione della performace individuale, misurazione della produttività, controllo dell'adempimento della prestazione lavorativa e profilazione del lavoratore.

Gli alert e le correlazioni generate automaticamente dal sistema saranno utilizzati esclusivamente per finalità di sicurezza informatica e non costituiranno autonomamente elementi di valutazione dell'operato del lavoratore.

Art. 4 – Accesso, utilizzo e conservazione dei dati

L'accesso ai dati generati e raccolti dal sistema SIEM è ammesso solo in presenza di uno specifico evento di sicurezza motivato e consentito esclusivamente a personale formalmente autorizzato dall'Azienda, dotato dei necessari profili di abilitazione e appositamente istruito in materia di protezione dei dati personali e sicurezza informatica. L'accesso potrà avvenire unicamente nei limiti e per le finalità specificamente indicate nelle premesse, in conformità ai principi di necessità, pertinenza e proporzionalità.

Ogni attività di accesso, consultazione, modifica o analisi dei dati presenti all'interno del sistema SIEM è tracciata, al fine di garantire la trasparenza e la verificabilità delle operazioni compiute, nonché il rispetto del principio del minimo privilegio.

Le attività ordinarie di analisi e monitoraggio saranno svolte, ove tecnicamente possibile, su dati aggregati o mascherati, anonimizzati solo quando non sia necessaria la successiva riconducibilità all'utente, oppure pseudonimizzati quando la re-identificazione sia indispensabile per la gestione degli incidenti di sicurezza. La consultazione nominativa o re-identificazione dell'utente potrà avvenire solo in presenza di uno specifico evento di sicurezza, con motivazione documentata, accesso autorizzato e tracciamento puntuale, limitatamente a quanto strettamente necessario.

La conservazione dei dati avverrà nei termini e secondo le modalità indicate nelle premesse, distinguendo tra i log centralizzati sul sistema SIEM (massimo 12 mesi) e i log conservati nei sistemi di origine (30, 90 o 180 giorni a seconda della tipologia). Decorso il periodo previsto, i dati saranno cancellati o resi non identificabili, in conformità al GDPR e alla normativa nazionale applicabile.

Art. 5 – Rendicontazione periodica accessi.

L'Azienda si impegna a trasmettere ai Coordinamenti delle Rappresentanze Sindacali Aziendali stipulanti il presente accordo, con cadenza semestrale, un report riepilogativo concernente gli accessi effettuati al sistema SIEM dal personale autorizzato, effettuate nell'ambito di verifiche di sicurezza non ordinarie.

Tale report, redatto in forma aggregata e nel rispetto della normativa vigente in materia di protezione dei dati personali, conterrà informazioni relative al numero degli accessi effettuati, con indicazione aggregata delle macro-finalità (es. incident response, verifica anomalie, attività di audit tecnico, gestione eventi di sicurezza), senza indicazione analitica dei dati trattati né diffusione di informazioni eccedenti rispetto alle finalità di trasparenza e monitoraggio condivise nel presente accordo.

Resta inteso che le informazioni condivise nell'ambito della presente previsione saranno utilizzate esclusivamente ai fini della verifica della corretta applicazione del presente accordo e del rispetto dei principi di necessità, pertinenza, proporzionalità e minimizzazione.

Il report non consentirà l'accesso diretto ai log, agli eventi di sicurezza, ai contenuti delle analisi tecniche o ai dati personali trattati nell'ambito delle attività di cybersecurity.

Art. 6 – Durata

Il presente accordo ha efficacia dalla data di sottoscrizione e rimarrà valido sino a diversa regolamentazione concordata tra le Parti.

Azienda e OO.SS. si incontreranno in ogni caso con frequenza almeno annuale per verificare la corretta applicazione dell'Accordo ed analizzare congiuntamente eventuali criticità emerse e valutare gli aggiornamenti normativi e regolamentari, nonché le eventuali modifiche tecniche o funzionali dei sistemi e degli applicativi utilizzati per la raccolta, la conservazione e il trattamento dei metadati, qualora rilevanti ai fini del presente Accordo.

Per il Gruppo Generali

Per le OO.SS.