ACCORDO DATA LOSS PREVENTION

Milano, 20 novembre 2025

Tra

Banco BPM, anche nella sua qualità di Capogruppo

e

la Delegazione Sindacale di Gruppo Banco BPM costituita dalle OO.SS. Fabi, First-Cisl, Fisac-CGIL, Uilca e Unisin Falcri-Silcea-Sinfub

Premesso che:

- la Data Loss Prevention (DLP) è una strategia di sicurezza informatica che utilizza strumenti e processi al fine di identificare, monitorare e proteggere dati sensibili da minacce interne o esterne per l'attività bancaria, per la gestione della clientela e dei relativi rapporti bancari;
- da parte aziendale è stata confermata l'esigenza di attivare strumenti di data loss prevention per il patrimonio dei dati aziendali così come definiti dal GDPR e, in particolare, rafforzare la capacità del Gruppo di intercettare possibili minacce interne ed esterne alla sicurezza dei dati aziendali, nel rispetto delle previsioni legislative tempo per tempo vigenti;
- l'Azienda garantisce che le soluzioni adottate, per le quali ha effettuato la valutazione di impatto ai sensi e nel rispetto dell'art. 35 GDPR, hanno le specifiche ed esclusive finalità di prevenzione del rischio di danno sopra definito e consentono la mitigazione delle ricadute derivanti dalla eventuale perdita o trasferimento non autorizzato (sottrazione) degli stessi, nel pieno rispetto dei principi previsti dalla normativa tempo per tempo vigente in materia di tutela della privacy (General Data Protection Regulation), con particolare riferimento ai principi di correttezza, liceità, trasparenza e minimizzazione nonché, qualora se ne ponesse l'esigenza, dei principi di cui all'art. 11 della Legge 132/2025;
- nell'ambito di appositi incontri l'azienda ha dichiarato che l'adozione dei meccanismi di funzionamento dei sopra citati strumenti, è finalizzata esclusivamente ad assicurare sempre più elevati presidi di sicurezza dei dati, derivanti dall'utilizzo degli strumenti informatici, nell'ottica di tutela di cui ai primi due alinea della presente premessa. L'azienda ha altresì dichiarato, con riferimento a quanto previsto dall'art. 4 della l. 300/1970, che tali strumenti ed i meccanismi di funzionamento adottati non potranno essere utilizzati per finalità di controllo a distanza delle lavoratrici e dei lavoratori e/o di monitoraggio e/o valutazione delle prestazioni lavorative. E' altresì escluso

ogni utilizzo di dati, strumenti e meccanismi per finalità disciplinari, ad eccezione dei casi di attività fraudolenta, esfiltrazioni dei dati e attacco cyber.

Articolo 1

Le premesse formano parte integrante del presente accordo.

Articolo 2

Gli strumenti di data loss prevention adottati dal Gruppo operano con modalità automatica unicamente durante lo scambio e la condivisione dei dati aziendali essenziali per l'attività bancaria e per la gestione della clientela e dei relativi rapporti bancari, all'interno e all'esterno del Gruppo stesso e nel rispetto dei principi in tema di protezione dei dati (GDPR) la cui integrale osservanza è garantita dalla parte aziendale in ogni fase di operatività degli strumenti. A tale riguardo, l'azienda dichiara che, la base giuridica per il trattamento dei dati è il legittimo interesse, previsto dall'art. 6, par. 1 lett F) GDPR.

Tenuto conto della finalità di cui in premessa, le rilevazioni del sistema di data loss prevention pervengono al personale autorizzato della funzione di sicurezza informatica del Gruppo.

Qualora, a fronte di alert relativi ad attività potenzialmente fraudolente si rendesse necessario visualizzare ed analizzare informazioni specifiche relative ad una singola utenza, potrà ad esse accedere, oltre all'autorità giudiziaria, il personale di cui al paragrafo che precede e il personale autorizzato delle funzioni controllo nel rispetto di ogni presidio in materia di riservatezza dei dati personali.

In caso di visualizzazione da parte del personale autorizzato delle funzioni di controllo e qualora emergessero elementi di attenzione riconducibili alla attività del dipendente, da parte aziendale sarà fornita comunicazione al dipendente interessato.

Il Gruppo si impegna a confrontarsi preventivamente con le OOSS in merito alla futura possibile attivazione di ulteriori strumenti informatici di data loss prevention o di aggiornamenti normativi che determinino la necessità di un'implementazione del presente accordo.

L'Azienda provvederà agli adempimenti di cui all'art. 4, comma 3, L. 300/1970 (adeguata informazione), agli artt. 13 e 14 GDPR nonché, qualora se ne ponesse l'esigenza, all'art. 4, comma 3 L. 132/2025, e ad aggiornare la normativa aziendale, in coerenza con quanto previsto dalla presente intesa.

L'azienda si impegna a fornire alle OO.SS., preventivamente alla sua

pubblicazione, il testo della circolare aziendale in tema di Data Loss Prevention, che costituirà informazione adeguata ai sensi dell'art. 4, comma 3, L. 300/1970 e dovrà contenere:

- finalità del trattamento
- tipologie di dati trattati
- modalità di funzionamento degli strumenti
- soggetti autorizzati al trattamento
- conservazione dei dati
- diritti dell'interessato
- base giuridica del trattamento
- contatti del Titolare e del DPO

Dichiarazione aziendale
Su richiesta del sindacato azienda conferma che i meccanismi sopra descritti di data loss prevention non danno luogo a nessuna tipologia di profilazione e/o decisione automatizzata.

Articolo 3

I dati vengono raccolti e trattati nel rispetto delle previsioni vigenti in materia di privacy, nonché conservati per il periodo definito dalle norme vigenti in materia di privacy o, in mancanza, per il periodo massimo di 12 mesi. Al termine del periodo indicato, i dati saranno automaticamente cancellati in modo irreversibile.

Dichiarazione delle Parti
L'Azienda si impegna ad effettuare interventi di informazione, formazione e aggiornamento per sensibilizzare i dipendenti in merito alle tematiche di DLP.

Banco BPM

anche in qualità di Capogruppo

Delegazione Sindacale - Gruppo Banco BPM

FABI FIRST CISL FISAC CGIL UILCA UNISIN FALCRI SILCEA SINFU