ACCORDO EX ART. 4 LEGGE N. 300 DEL 1970

DATA LEAKAGE PREVENTION

Il giorno 30 luglio 2021

Tra

ING Bank N.V. – Succursale di Milano (di seguito anche la "**Banca**" o "**ING**")

E

Le **Organizzazioni Sindacali** rappresentate dalle rispettive RSA (di seguito anche le "**OOSS**" e, congiuntamente alla Banca, le "**Parti**")

FABI

FIRST CISL

FISAC CGIL

UILCA

UNISIN

Premesso che

- La Banca, nello svolgimento delle proprie attività, elabora e archivia rilevanti quantità di informazioni riservate tra cui, a titolo esemplificativo e non esaustivo, informazioni di identificazione personale (*Personally Identifiable Information*), dati bancari e informazioni riferite alle transazioni eseguite dalla clientela, dati di fornitori/terze parti coinvolte a vario titolo nella gestione di porzioni, anche significative, di processi di business nonché dati di rilevanza strategica;

- L'esperienza recente dimostra che:
  a. con l'aumento del volume dei dati digitali e la diversificazione di applicazioni e piattaforme si è registrata una diffusione capillare dei dati, ora anche in *cloud*, ed il controllo sugli accessi ai dati è divenuto notevolmente più complesso;
  b. l'incremento della potenza di elaborazione dei c.d. *endpoint* (i.e. computer/laptop/dispositivo mobile aziendale che contiene i dati stessi o recupera le informazioni da un servizio/server/applicazione) ha portato un maggior numero di utenti a visualizzare, scaricare e analizzare dati in modo decentralizzato e ad archiviarne i risultati all'interno di "community" di utenti finali;
  c. file e documenti non strutturati possono contenere grandi quantità di dati di identificazione personale o altre informazioni di proprietà dalla Banca;
  d. i clienti e le terze parti accedono ai dati di ING tramite Internet e/o applicazioni per utenti finali rendendo labile la distinzione tra accessi interni ed esterni.

- Anche a seguito di espressa segnalazione rivolta al Gruppo ING da parte della Banca Centrale Europea di implementare un sistema volto ad evitare la perdita di dati e il trasferimento non autorizzato di informazioni riservate, la Banca ha quindi la necessità di porre in essere verifiche al fine di prevenire la perdita di dati ed informazioni riservate, ivi inclusi i dati personali dei propri clienti, dipendenti e

terze parti, tramite browser web, servizi di posta elettronica, dispositivi di archiviazione e dispositivi di stampa e quindi ad evitare l'applicazione di sanzioni normative da parte delle Autorità competenti, danni reputazionali e perdite economiche;

- la necessità di adottare adeguate misure tecniche e organizzative di sicurezza al fine di prevenire la perdita di confidenzialità, integrità e disponibilità anche di dati personali (circostanze che potrebbero ingenerare eventi di *data breach*) è, altresì, dettata dal Regolamento (UE) 2016/679 (cd. "GDPR") all'art. 32 (sicurezza del trattamento). Inoltre, l'adozione di appropriate misure di prevenzione e controllo ha lo scopo di consentire alla Banca di adempiere correttamente alle obbligazioni poste a proprio carico dagli artt. 33 e 34 del GDPR qualora si verifichi una violazione dei dati personali che ponga a rischio i diritti e le libertà fondamentali degli interessati;

- in questo contesto, la Banca ha dunque deciso di introdurre ed implementare un sistema di controllo c.d. "**Data Leakage Prevention**" (di seguito, "**DLP**") per prevenire, monitorare e bloccare l'eventuale perdita e l'esfiltrazione non autorizzata di dati aziendali, ivi inclusi i dati personali dei propri clienti, dipendenti e terze parti (di seguito, i "**Dati Aziendali**"), tramite i diversi canali di comunicazione impiegati dalla Banca, tra cui browser web, servizi di posta elettronica, dispositivi di archiviazione e dispositivi di stampa;

- il sistema **DLP** è volto ad intercettare la perdita ed esfiltrazione non autorizzata di Dati Aziendali ed è dunque determinato da esclusive ragioni di sicurezza del lavoro e di tutela del patrimonio informatico e informativo aziendale previste dall'art. 4, comma 1, della legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), non comportando alcuna forma di controllo a distanza e/o di monitoraggio dell'attività lavorativa;

- inoltre, l'adozione del sistema **DLP** e la definizione delle relative regole di gestione avverranno conformemente a quanto stabilito dalla "*Policy sull'Utilizzo degli Strumenti Elettronici Aziendali*" adottata e comunicata dalla Banca a tutti i dipendenti, nonché nel rispetto delle "*Linee Guida del Garante per la Posta Elettronica e Internet*" emanate dal Garante per la Protezione dei Dati Personali il 10 Marzo 2007;

- il trattamento dell'esigua quantità di dati personali dei dipendenti (v. infra par. "*informazioni registrate e conservate*") processati nell'ambito dell'utilizzo del sistema **DLP** avverrà in conformità alle vigenti disposizioni in materia;

- la Banca e le OOSS, condivise le esigenze di sicurezza e di tutela del patrimonio aziendale sopra descritte, anche nell'ottica di favorire la regolarità ed efficienza dello svolgimento delle attività lavorative, sottoscrivono il presente accordo ai sensi dell'art. 4, della l. n. 300/1970 sopra citata (di seguito, anche l'"**Accordo**").

Tutto ciò premesso, le Parti convengono quanto segue.

Premesse

1. Le premesse formano parte integrante del presente Accordo.

Il sistema Data Leakage Prevention (DLP): definizione e finalità

2. A partire dal 1 settembre 2021 presso la Banca viene implementato un sistema identificato come **Data LeakagePrevention (DLP)**, avente ad oggetto il controllo:
    - del caricamento (*upload*) di documenti tramite browser web;
    - dell'invio di documenti a mezzo posta elettronica aziendale (sono quindi espressamente esclusi i controlli sulle comunicazioni provenienti da fonti esterne in entrata sull'indirizzo di posta elettronica aziendale);

- della scrittura di *file* su supporti rimovibili, laddove tale ipotesi sia consentita dalle policy aziendali tempo per tempo vigenti, e/o sistemi di archiviazione remota;
- della stampa di documenti tramite la funzione corrispondente dei sistemi operativi;

al fine di bloccare e/o registrare la perdita e l'esfiltrazione di Dati Aziendali non autorizzati ad opera dei dipendenti per il tramite dei predetti canali aziendali in dotazione nello svolgimento dell'attività lavorativa (di seguito "**Endpoint**"). La Banca dichiara che il sistema **DLP** dalla stessa identificato è "McAfee DLP".

3. Il sistema **DLP** è volto, in coerenza con quanto stabilito pure dalla "*Policy sull'Utilizzo degli Strumenti Elettronici Aziendali*" adottata dalla Banca nonché nel rispetto delle "*Linee Guida del Garante per la Posta Elettronica e Internet*", ad intercettare la perdita ed esfiltrazione non autorizzata di Dati Aziendali dagli Endpoint ed è dunque determinato da esclusive ragioni di sicurezza del lavoro e di tutela del patrimonio informatico e informativo aziendale previste dall'art. 4, comma 1, della legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), non comportando alcuna forma di controllo a distanza e/o di monitoraggio dell'attività lavorativa e non essendo utilizzato ai fini della valutazione professionale dei lavoratori, ai sensi delle normative vigenti.

Funzionamento del sistema Data Leakage Prevention (DLP)

4. Il sistema **DLP** è finalizzato a controllare il caricamento (*upload*) di documenti tramite browser web, l'invio di documenti a mezzo posta elettronica aziendale, la scrittura di file su supporti rimovibili - laddove tale ipotesi sia consentita dalle policy aziendali tempo per tempo vigenti - e/o sistemi di archiviazione remota e la stampa di documenti tramite la funzione corrispondente dei sistemi operativi e ad intercettare le seguenti categorie di informazioni e dati riferite a clienti, dipendenti e terze parti contenute negli Endpoint, la cui presenza ed utilizzo determina l'insorgere di un *alert* relativo alla perdita ed esfiltrazione di Dati Aziendali non autorizzati:
    a. documenti e/o informazioni con classificazione C3 sulla base delle policy aziendali vigenti (i.e. documenti e/o informazioni di natura confidenziale riferite, a titolo esemplificativo e non limitativo, alle posizioni e/o ai prodotti dei Clienti, ai dati dei dipendenti della Banca, ai dati afferenti alla gestione e organizzazione di attività rilevanti per il business di ING, ecc.);
    b. documenti e/o informazioni con classificazione C4 sulla base delle policy aziendali vigenti (i.e. documenti e/o informazioni di natura segreta riferite, a titolo esemplificativo e non limitativo, ai dati di natura sensibile/particolare dei Clienti e/o dipendenti della Banca, ai dati afferenti alla determinazione e gestione delle strategie di business identificate da ING per il perseguimento del proprio oggetto sociale, ai dati di natura economico/finanziaria prima che la divulgazione dei medesimi sia consentita sulla base dei processi Banca e delle strategie di mercato di ING, ecc.).

I monitoraggi tramite il sistema **DLP** sono eseguiti sulla base di regole di configurazione dell'applicativo che hanno lo scopo di intercettare, mediante una serie di logiche associative, meccanismi di settaggio ed algoritmi, la presenza di informazioni connesse a Dati Aziendali riconducibili alle categorie di confidenzialità C3 o C4 sopra descritte, senza però che ciò possa in alcun modo comportare la possibilità per il sistema **DLP** di leggere, analizzare e memorizzare il contenuto delle comunicazioni medesime ovvero senza eseguire un controllo specifico su singole utenze. In altre parole, sulla base delle configurazioni eseguite il sistema **DLP** potrà dare un output di ritorno sotto forma di alert qualora informazioni classificabili come C3 o C4 vengano processate, senza che nella fase preliminare di utilizzo del DLP il contenuto delle singole comunicazioni possa essere conosciuto o conoscibile da parte della Banca.

Laddove nell'ambito delle verifiche di cui al punto 6. che segue, venisse accertato che l'evento generante l'alert è un cd. "falso positivo", non verrà dato seguito ad alcuna ulteriore analisi da parte della Banca. A titolo esemplificativo e non esaustivo, si considera un "falso positivo" l'invio a mezzo email tra colleghi di informazioni C3 e/o C4 reso necessario dall'attività lavorativa espletata nella sua più ampia accezione.

5. In particolare, una volta rilevato dal sistema **DLP** anche tramite parole chiave l'invio/il caricamento di uno o più dei documenti/informazioni contenenti elementi riconducibili alle categorie di confidenzialità C3 o C4, a seconda del grado di riservatezza e confidenzialità dei Dati Aziendali e dell'Endpoint in cui gli stessi sono contenuti, il sistema stesso può:
    a. bloccarne l'invio/il caricamento/la stampa con generazione di *alert*;
    b. generare un *pop-up* preventivo che richiede all'utente di indicare la ragione per cui si intende procedere all'invio/caricamento/la stampa dei documenti/delle informazioni e dei dati in questione con conseguente generazione di *alert*;
    c. generare un *alert*, consentendo all'utente l'invio/caricamento/la stampa dei documenti/delle informazioni e dei dati in questione.

6. Al fine di bloccare o registrare le azioni che vengono eseguite, nei casi descritti al punto 5. che precede il sistema **DLP** invia un *alert* al sistema di monitoraggio "GSOC" (Global Security Operating Center) di ING Services Polska. Gli analisti del GSOC di ING Services Polska verificano l'*alert* e, se necessario, lo trasmettono al team CISO (Chief Information Security Office) locale della Banca al fine di effettuare le opportune verifiche.

Tipologia di strumenti di lavoro soggetti a Data Leakage Prevention

7. Gli strumenti di lavoro aziendali attraverso i quali potrà darsi luogo al controllo **DLP** sono Internet e la posta elettronica aziendale (utilizzabili dal PC, dallo *smartphone* e dal *tablet*), i dispositivi di archiviazione e le stampanti di rete. Laddove la Banca dovesse mettere a disposizione per i lavoratori eventuali altri dispositivi per lo svolgimento dell'attività lavorativa la Banca informerà preventivamente le OOSS prima di sottoporli al controllo DLP, laddove necessario.

Informazioni registrate e conservazione

8. Le informazioni che verranno registrate nell'ambito della generazione dell'*alert* sono le seguenti:
    - data ed ora di accadimento dell'evento;
    - tipologia e *severity* dell'evento;
    - nome della *workstation*;
    - indirizzo IP;
    - e-mail (informazione catalogabile come dato personale);
    - *corporate key* (informazione catalogabile come dato personale);
    - applicazione sulla quale è stato rilevato l'evento;
    - nome e dimensioni del *file* che ha generato l'evento;
    - soggetti a cui è stata trasmessa l'e-mail (in caso di e-mail), sito web sul quale è avvenuto il caricamento del documento (in caso di caricamento via web);
    - oggetto della e-mail (in caso di e-mail);
    - classificazione rilevata dal sistema DLP;
    - eventuale giustificazione fornita dall'utente;
    - parola chiave che ha generato l'*alert,* senza che tale parola chiave possa in alcun modo rivelare in tutto o in parte il contenuto della comunicazione.

    Ad ogni modo, come evidenziato anche al par. *"Funzionamento del sistema Data Leakage Prevention"*, si ribadisce che il sistema **DLP** in nessun caso monitora e conserva i contenuti delle informazioni condivise (per es. il contenuto dell'e-mail inviata all'esterno), ma memorizza solo la traccia della presenza di informazioni classificabili come C3 o C4 all'interno di una comunicazione che ha generato l'*alert* e, dunque, fatto scattare la regola di controllo.

9. Nel caso si ravvisasse la necessità di registrare ulteriori tipologie di informazioni rispetto a quelle qui elencate, le integrazioni saranno tempestivamente e preventivamente oggetto di specifico incontro con le OOSS.

10. Le informazioni raccolte dal sistema **DLP** vengono registrate su supporto digitale e conservate all'interno del server centrale di ING collocato, nelle sue varie dislocazioni, interamente nel territorio dell'Unione Europea. Tale conservazione viene mantenuta per i 6 mesi successivi alla raccolta, fatte salve speciali esigenze di ulteriore conservazione in relazione al caso in cui si dovrà aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria o per esigenze di esercizio del diritto di difesa in giudizio o su richiesta delle Autorità di Vigilanza. Decorso tale periodo i dati raccolti verranno cancellati.

11. Le informazioni raccolte dal sistema DLP sono accessibili al personale autorizzato, facente parte dell'area CISO locale della Banca, il quale vi accede attraverso profili di accesso specifici e personali. Le predette informazioni sono accessibili anche alle aree CISO globale, IRM (Information Risk Management) globale, CIRM (Corporate Information Risk Management) globale e CSI (Corporate Security & Investigations) globale.

12. In particolare, qualora si inneschi un *alert,* e fermo quanto previsto al punto 6. che precede, gli addetti all'area CISO e IRM locale potranno richiedere tempestivamente a mezzo e-mail le informazioni relativamente all'*alert* al dipendente che ha provveduto all'invio/caricamento/stampa di documenti/informazioni/dati tramite l'Endpoint che ha generato l'*alert* informando contestualmente anche il relativo Responsabile. Il dipendente interessato sarà tenuto a fornire prontamente un motivato riscontro e potrà richiedere supporto al Responsabile stesso.

13. Nei casi in cui si rendessero necessari ulteriori chiarimenti e verifiche, rispetto a quanto previsto al punto 12. che precede, il dipendente potrà inoltre essere sentito dagli addetti dell'area CISO e IRM locale nell'ambito di un apposito incontro concordato preventivamente. In questa sede il dipendente interessato avrà la possibilità di richiedere l'assistenza di un rappresentante sindacale.

14. Nelle fasi di cui ai punti 12. e 13. che precedono, laddove necessario, il trattamento degli eventuali dati personali dei dipendenti coinvolti avverrà nel rispetto di quanto indicato nell'informativa *privacy* consegnata ai dipendenti in fase di assunzione e s.m.i. L'informativa *privacy* tempo per tempo applicabile è consultabile nella sezione "HR" della Intranet Aziendale.

15. I dati registrati dal sistema di cui al presente Accordo non verranno in alcun modo utilizzati per l'adozione di provvedimenti disciplinari, a meno che dagli accertamenti non emergano comportamenti dolosi o gravemente colposi o attuati in violazione di specifiche normative regolamentari, contrattuali e/o di legge. In particolare, la colpa grave dovrà essere contraddistinta da un comportamento tale da escludere la casualità dell'evento, e che comporti un danno oggettivo e dimostrabile di carattere rilevante per la Banca.

    DICHIARAZIONI OOSS:
    Le OOSS invitano la Banca a non adottare provvedimenti disciplinari nei confronti dei lavoratori per tutte le casistiche rivenienti dagli accertamenti di cui sopra e ricadenti nella colpa grave, qualora commesse nell'esercizio delle proprie mansioni ovvero per finalità strettamente lavorative.

Varie

16. Le Parti convengono altresì che ove si verificasse la necessità di apportare significative modifiche e/o integrazioni al suddetto sistema, la Banca ne darà preventiva comunicazione alle OOSS. Le Parti valuteranno congiuntamente l'eventuale necessità di modificare o integrare l'Accordo stesso.

17. La Banca si impegna ad informare i lavoratori in ordine al sistema **DLP**, anche attraverso la consegna a mezzo e-mail di specifica informativa sul trattamento dei dati personali redatta in conformità alla vigente normativa - secondo il format che verrà condiviso preventivamente dalla Banca alle OOSS - nonché tramite adeguate comunicazioni almeno annuali di sensibilizzazione sui temi afferenti alla corretta gestione delle informazioni processate dalla Banca.

18. Dal momento dell'entrata in vigore del presente Accordo, si stabilisce un periodo iniziale di osservazione della durata di 3 mesi a partire da settembre, durante il quale sono sospesi temporaneamente gli effetti disciplinari previsti dal punto 15. fatti salvi i casi di dolo.

19. Entro un anno dalla data di sottoscrizione del presente Accordo, e successivamente con cadenza annuale, le Parti effettueranno un incontro di verifica per valutare gli effetti della sua applicazione nonché l'evoluzione del contesto normativo.

20. Le Parti si danno atto che, con la sottoscrizione del presente accordo, è stata validamente esperita e completata la procedura di cui all'art. 4, comma 1, L. n. 300/70.

Letto, firmato e sottoscritto

Milano, 30 luglio 2021

RSA FABI

ING Bank N.V. – Succursale di Milano

RSA FIRST CISL

RSA FISAC CGIL

RSA UILCA

RSA UNISIN