VERBALE DI ACCORDO

AI SENSI DELL'ART 4 LEGGE 20 MAGGIO 1970 N. 300

DATA LOSS PREVENTION

Il giorno 8 settembre 2022

hanno partecipato alla riunione:

la Società:

- Santander Consumer Bank S.p.A. in persona di:
  Guido Piacenza - Direttore del Servizio Risorse Umane e Organizzazione
  Paola Amerio – HR Business Partner e Relazioni Industriali;

e

le OO.SS.

- FABI rappresentata da:
  Alberto D'Andrea (Segretario di Coordinamento)
- FISAC CGIL rappresentata da:
  Marcello Carcereri (Segretario di Coordinamento)

Premesso che:

- Santander Consumer Bank ha comunicato la necessità di predisporre adeguati strumenti di tutela delle informazioni tramite strumenti volti alla prevenzione della perdita di dati (Data Loss Prevention);
- L'Azienda ha rimarcato che le informazioni, le conoscenze e il *know how* contenuti in tali dati costituiscono una risorsa fondamentale per lo sviluppo dei propri prodotti e dei relativi business e si rivela pertanto necessario proteggerli dai rischi di perdita accidentale, dispersione, diffusione impropria;
- 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, 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;
  1. Al verificarsi dell'aumento del volume dei dati digitali e della diversificazione di applicazioni e di piattaforme si registra una diffusione capillare dei dati, anche in cloud. Il controllo sugli accessi ai dati è divenuto notevolmente più complesso;
  2. 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 e ad archiviarne i risultati all'interno della nostra rete interna;
  3. Tali file e documenti possono contenere grandi quantità di dati di identificazione personale o altre informazioni di proprietà dalla Banca;
  4. Le terze parti possono accedere ai dati della Banca tramite Internet e/o applicazioni aziendali, rendendo labile la distinzione tra accessi interni ed esterni.

- Anche a seguito di espresso mandato dal Gruppo Santander 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 aziendali, 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 Loss 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, *Endpoint* (PC, Smartphone, Stampanti) e Cloud;
- 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 e in osservanza a quanto previsto dal Garante Privacy nelle *"Linee guida del Garante per posta elettronica e internet"* (Gazzetta Ufficiale n. 58 del 10 marzo 2007);
- Inoltre, l'adozione del sistema **DLP** e la definizione delle relative regole di gestione avverranno conformemente a quanto stabilito dalle Policy *"Cyber Security Requirements for Business Areas", "Cyber Security Requirements for Technical Users" e "Regole di Comportamento per la Cyber Security"* adottate e comunicate 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;
- L'Azienda ha comunicato la necessità di procedere, al fine di rispondere alle finalità sopra descritte ed in linea con le migliori pratiche adottate dalle aziende leader nei loro settori di riferimento, all'installazione di un sistema di protezione e prevenzione della perdita, dispersione e diffusione impropria dei dati (c.d. data loss prevention), fornito attraverso i servizi di DLP erogati dal Gruppo Santander che includono l'installazione di software specifici sui canali precedentemente citati;
- Il servizio DLP è già attivo con esito positivo presso diverse società del Gruppo Santander;
- l'art. 4 della legge 20 maggio del 1970, n. 300, così come modificato dal decreto legislativo. 151 del 14 settembre 2015 e dal decreto legislativo n. 185 del 24 settembre 2016 e che qui integralmente si richiama prevede, tra l'altro, che gli strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere installati previo accordo collettivo stipulato, nel caso di imprese con unità produttive ubicate in diverse province della

stessa regione ovvero in più regioni, dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale;

Ciò premesso, e considerato,

le Parti convengono che le Premesse costituiscono parte integrante del presente Accordo.

Art. 1
DLP: definizione e finalità

A partire dal 19/09/2022 presso la Banca verrà implementato un servizio identificato come **Data Loss Prevention (DLP)**, avente ad oggetto il monitoraggio e controllo dei canali browser web, posta elettronica, *Endpoint* (PC, Smartphone, Stampanti), dispositivi di archiviazione e Cloud come indicato nello Standard *"CS-ST-015_DLP_Controls"*. A titolo esemplificativo:

- il caricamento (*upload*) di documenti tramite applicazioni web diverse da quelle approvati da Santander (es. OneDrive);
- l'invio di documenti/dati a mezzo posta elettronica aziendale verso indirizzi esterni (sono quindi espressamente escluse dai controlli DLP le comunicazioni in entrata sull'indirizzo di posta elettronica aziendale);
- l'utilizzo di supporti rimovibili, conformemente alle policy aziendali tempo per tempo vigenti;
- la stampa di documenti in base alla loro classificazione.

Art. 2
DLP: policy interne

Il sistema **DLP** è volto, in coerenza con quanto stabilito dalle policy *"Cyber Security Requirements for Business Areas", "Cyber Security Requirements for Technical Users" e "Regole di Comportamento per la Cyber Security"* adottate 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.

Art. 3
DLP: funzionamento

1. Il sistema **DLP** è finalizzato all'esecuzione dei controlli descritti nell'Art.1 (*CS-ST-015_DLP_Controls)* e in funzione delle categorie di dati riferite a clienti, dipendenti e terze parti, come indicati nelle policy *"Cyber Security Requirements for Business Areas", "Cyber Security Requirements for Technical Users"* e nello Standard "CS-ST-007-*Data Security Classification Standard"*, ovvero:

   Il servizio di **DLP** prevede la configurazione dei sistemi che lo costituiscono in modo che intercetti le casistiche descritte nel documento *"CS-ST-015_DLP_Controls"*.

Il servizio **DLP** sarà pertanto in grado di riconoscere, in base alla classificazione del dato e dell'attività che si vuole svolgere (upload, stampa, copia, trasferimento, modifica/cancellazione) un potenziale rischio di perdita di dati. In tal caso sarà registrato un *alert* di sicurezza in una apposita ***Console DLP***.

In altre parole, sulla base delle configurazioni effettuate, il sistema **DLP** potrà fornire un output di ritorno sotto forma di *alert*, qualora si presentino le casistiche previste nel documento *"CS-ST-015_DLP_Controls"*, senza che nella fase preliminare di utilizzo del DLP il contenuto delle singole operazioni possa essere conosciuto o conoscibile da parte della Banca.

Laddove nell'ambito delle verifiche di cui al punto 3. 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" lo scambio di dati a mezzo E-mail tra Società appartenenti al Gruppo Santander.

2. In particolare, una volta rilevato dal servizio **DLP** una delle casistiche descritte nel documento *"CS-ST-015_DLP_Controls"* , il servizio stesso genera un *alert* e può:
   a) generare un *pop-up* preventivo che richiede all'utente di indicare la ragione per cui si intende procedere con l'operazione (stampa, invio, copia...);
   b) bloccare l'operazione;
   c) consentire l'operazione.

3. Al fine di bloccare o registrare le operazioni che vengono eseguite, il sistema **DLP** invia un *alert* al Servizio "SOC" (Security Operating Center) del Gruppo Santander che verificherà l'*alert* e, se necessario, lo trasmetterà al team CISO (Chief Information Security Office) locale della Banca al fine di effettuare le opportune verifiche.

4. Tutti gli *alert* e i dati caratterizzanti l'evento che li ha generati sono visibili all'interno della ***Console DLP***, a cui ha accesso il CISO locale della Banca per la loro gestione per dieci anni.

Art. 4
Strumenti di lavoro soggetti DLP

Gli strumenti di lavoro aziendali attraverso i quali potrà darsi luogo al controllo **DLP** sono Internet, posta elettronica, Endpoint (PC, Smartphone, Stampanti), dispositivi di archiviazione e Cloud. 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.

Art. 5
Informazioni registrate e conservazione

Le informazioni che verranno registrate nell'ambito della generazione dell'*alert* sono le seguenti:

- Regola che ha innescato l'evento;
- Data ed ora di accadimento dell'evento;
- Tipologia e severity dell'*alert*;
- Nome e indirizzo IP della workstation associata all'evento;
- Username (informazione catalogabile come dato personale);

- Sito web sul quale è avvenuto il caricamento del documento (in caso di caricamento via web);
- Mittente e-mail (informazione catalogabile come dato personale);
- Destinatari a cui è stata trasmessa l'e-mail (in caso di e-mail);
- Files coinvolti nell'evento con visibilità di nome, dimensioni e contenuto; Applicazione utilizzata (es. Outlook.exe).

1. Le informazioni raccolte dal sistema **DLP** vengono registrate su supporto digitale e conservate all'interno dei sistemi utilizzati dal Servizio SOC collocato nel territorio dell'Unione Europea. Tale conservazione viene mantenuta per i dieci anni successivi alla raccolta. Decorso tale periodo i dati raccolti verranno cancellati.
2. Le informazioni raccolte dal sistema DLP sono accessibili al personale autorizzato, facente parte dell'area **CISO** locale della Banca (eccetto i contenuti dei file collegati all'evento), del Data Protection Officer (compreso il contenuto dei file) e di funzioni specifiche di Capogruppo (GLOBAL PROTECT, per attività di amministrazione del sistema e GLOBAL SOC, per l'analisi degli alert e delle policy del DLP). Gli accessi si svolgono attraverso credenziali di accesso personali e profili specifici.

3. In particolare, qualora si inneschi un *alert,* gli addetti dell'area CISO locale potranno richiedere tempestivamente, all'utente che ha effettuato l'operazione e che ha generato l'alert, delle spiegazioni informando anche il relativo Responsabile. Il dipendente interessato sarà tenuto a fornire prontamente un motivato riscontro e potrà richiedere supporto al Responsabile stesso.

4. Nei casi in cui si rendessero necessari ulteriori chiarimenti e verifiche, o in assenza di riscontri, il dipendente potrà inoltre essere sentito dagli addetti dell'area CISO e DPO (Data Protection Officer) insieme alla Direzione Risorse Umane 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.

5. Laddove necessario, il trattamento degli eventuali dati personali dei dipendenti coinvolti avverrà nel rispetto di quanto indicato nell'informativa *privacy* consegnata, a puro scopo informativo, ai dipendenti in fase di assunzione e come da eventuali successive modifiche e integrazioni.

6. 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.

Art. 6
Varie

1. 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.

2. La Banca, nonostante l'interesse legittimo quale base dell'attività di Data Loss Prevention, si impegna ad informare i lavoratori in ordine al sistema **DLP**, tramite specifica informativa sul trattamento dei dati personali redatta in conformità alla vigente normativa nonché tramite adeguate comunicazioni di sensibilizzazione sui temi afferenti alla corretta gestione delle informazioni processate dalla Banca.
3. 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 (ottobre?) 2022, durante il quale sono sospesi temporaneamente gli effetti disciplinari fatti salvi i casi di dolo.
4. 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.

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 e sottoscritto:

SANTANDER CONSUMER BANK SPA

Direttore Risorse Umane
GUIDO PIACENZA

HRBP e Relazioni Sindacali
PAOLA AMERIO

ORGANIZZAZIONI SINDACALI

(FABI) Alberto D'Andrea

(FISAC CGIL) Marcello Carcereri