**VERBALE D'INTESA**

In data 21 ottobre 2019, in Sondrio

tra

- la **Banca Popolare di Sondrio s.c.p.a.** che interviene in qualità di Capogruppo anche in nome e per conto di Banca della Nuova Terra, rappresentata dal signor Luigino Negri, Responsabile Servizio Personale;

e

- **delegazione sindacale** prevista ai sensi e per gli effetti del combinato disposto dell'art. 22 del c.c.n.l. 31 marzo 2015 e dell'art. 25 dell'accordo in materia di agibilità sindacali del 25 novembre 2015 e formata dalle seguenti Organizzazioni Sindacali **UNISIN e FIRST - CISL,**

**Premesso che**

Banca Popolare di Sondrio ha dichiarato che, a fronte della necessità di predisporre idonei strumenti di difesa volti a garantire il rigoroso rispetto delle previsioni normative vigenti, in tema di protezione dei dati, da ultimo il General Data Protection Regulation (GDPR) entrato in vigore il 25 maggio 2018, e della forte e continua evoluzione delle modalità di attacco tramite sistemi informatici, in un'ottica di mitigazione del rischio informatico a cui BPS è potenzialmente esposta, si rende necessario e opportuno adottare nuove soluzioni informatiche, finalizzate a tutelare la privacy dei soggetti interessati e la protezione dei dati rilevanti per la Banca Popolare di Sondrio, che consentano l'individuazione di anomalie di sicurezza non riconducibili dai sistemi tradizionali oggi utilizzati.

Le predette soluzioni sono quindi finalizzate a minimizzare i rischi relativi alla sicurezza del patrimonio aziendale e dei dati trattati aziendalmente, rafforzando la capacità di intercettare possibili minacce provenienti da utenti interni ed esterni con l'obiettivo di prevenire la perdita di informazioni a causa di errore umano o potenziale utilizzo non legittimo dei dati.
Il presidio di sicurezza aziendale sarà implementato integrando gli attuali sistemi di sicurezza con la soluzione informatica di analisi dei dati aziendali (Symantec Data Loss Prevention Solution) descritta alle Organizzazioni Sindacali (e sinteticamente nell'allegato tecnico) e adeguando conseguentemente i processi interni di controllo.

**considerato che**

l'art. 4 della legge 300/70 recita che gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo con le associazioni sindacali comparativamente più rappresentative sul piano nazionale.

La Banca intende adottare tale accordo anche per la controllata Banca della Nuova Terra Spa a cui Banca Popolare di Sondrio fornisce, con specifici accordi di servizio, infrastrutture tecnologiche, sistemi e applicativi informatici.

La Banca ha dichiarato che l'introduzione della nuova soluzione "Symantec Data Loss Prevention" è indispensabile per garantire il livello di sicurezza adeguato al rischio di trattamento dei dati consentendo di rilevare e prevenire comportamenti anomali e/o sconosciuti da parte di: utenti interni (dipendenti), di soggetti esterni (terze parti con cui BPS collabora) o di attacchi esterni (hackers), che si possono concretizzare in incidenti informatici a vario livello che le soluzioni di sicurezza tradizionali non sono in grado di rilevare o prevenire.
La Banca ha dichiarato che l'adozione delle misure oggetto della presente intesa è motivata esclusivamente dalla necessità di perseguire un sempre più elevato presidio di sicurezza del complesso patrimonio aziendale e dei dati personali derivanti dall'utilizzo di tecnologie informatiche, in aderenza anche alle indicazioni delle Autorità europee in tema di protezione dei dati personali e di cyber security.

Alle aziende è espressamente richiesto dalle normative vigenti di mettere in atto processi che garantiscano e tutelino la privacy, minimizzando i relativi rischi per i diritti e le libertà dei soggetti interessati.

**Tutto ciò premesso si conviene quanto segue:**

Art. 1

Le premesse formano parte integrante del presente accordo.

Art. 2

La Banca ha dichiarato che la soluzione di "Symantec Data Loss Prevention" che intende adottare, consentirà il monitoraggio, con modalità automatiche e semi automatiche, dell'intero traffico dati interno ed esterno all'azienda (compresa la posta elettronica) e sarà finalizzata a minimizzare i rischi associati al trattamento dei dati evidenziando comportamenti e modalità di utilizzo di tutti i dispositivi connessi alla rete aziendale non conformi alle disposizioni normative, anche aziendali, sulla protezione dei dati.

I dati, salvo quanto previsto dai successivi articoli, saranno trattati solo per le finalità di sicurezza di cui nelle premesse e per il periodo strettamente necessario a tali scopi (indicativamente due anni, fatte salve tutte le normative di specie), escludendo qualsiasi attività di monitoraggio del lavoratore o gruppi di lavoratori.
Le notifiche di sicurezza fornite dal sistema verranno sottoposte ad una prima analisi tecnica da parte della Funzione di Sicurezza aziendale che verificherà l'effettiva presenza di anomalie rispetto ai modelli previsti.
Qualora l'anomalia fosse ricondotta ad un incidente di sicurezza, verrà avviato uno specifico processo di gestione integrato con il processo di gestione degli incidenti aziendali.
Le analisi effettuate forniranno ulteriore supporto alle consuete e più ampie attività di analisi dei rischi informatici effettuate dalla Banca, consentendo di perfezionare l'efficacia delle misure e dei presidi di sicurezza a tutela del patrimonio informativo aziendale e degli stessi lavoratori.
La Banca dichiara che l'utilizzo delle soluzioni DLP di cui al presente accordo è aderente alle norme in materia di privacy, ivi compresi il General Data Protection Regulation; in particolare, i dati, compresi i log relativi alle anomalie riscontrate saranno conservati in stretta osservanza delle norme previste dal GDPR e dalla normativa di riferimento tempo per tempo vigente.

Art. 3

Qualora si rendesse necessario visualizzare ed analizzare informazioni specifiche relative ad una singola utenza, questo potrà avvenire esclusivamente da parte di dipendenti dell'Ufficio Sicurezza ICT, della Revisione interna oltre che dalle Forze dell'Ordine. La visualizzazione e l'analisi delle informazioni della singola utenza potranno avvenire esclusivamente per le finalità, sopra descritte, di sicurezza del complessivo patrimonio aziendale, della tutela della clientela e della protezione dei dati, restando pertanto escluso ogni utilizzo delle informazioni ottenibili ai fini della valutazione delle prestazioni dei dipendenti sotto il profilo sia quantitativo, sia qualitativo, né a fini disciplinari, fatti salvi i casi di dolo e colpa grave.

Art. 4

Qualora, a seguito delle attività di cui al precedente articolo 3, emergessero elementi di attenzione riconducibili alle attività di un dipendente che possano avere anche rilevanza ai fini disciplinari, il Servizio Personale fornirà le necessarie comunicazioni al dipendente interessato. Quest'ultimo potrà richiedere la visione degli elementi rilevati e farsi assistere da un Rappresentante di una delle Organizzazioni Sindacali firmatarie del presente accordo.
Quanto previsto al comma che precede avverrà in forma preventiva rispetto alle procedure dall'art. 7 della legge 300/70.

Art. 5

Per l'attuazione dell'adeguata informazione di cui al comma 3 dell'art. 4 legge 300/70, si provvederà all'aggiornamento delle policy, anche alla luce delle eventuali novità normative e si utilizzeranno i consueti canali di comunicazione aziendale (portale intranet, circolari, ordini di servizio ecc.).

Art. 6

La Banca si impegna a tenere informate le Rappresentanze sindacali su ulteriori ed eventuali sistemi/applicativi informatici che, in futuro, si volessero adottare in conformità ai principi indicati nel presente accordo.

Letto, approvato e sottoscritto.

BANCA POPOLARE DI SONDRIO
(in qualità di Capogruppo, anche in nome e per conto di Banca della Nuova Terra)

LE RAPPRESENTANZE
SINDACALI

Carlo Dell'Oca

**Allegato accordo sindacale del 21 ottobre 2019 sui sistemi informatici per il monitoraggio del traffico dati interno e esterno**

Gli strumenti informatici di Data Loss Prevention and Protection, e/o content filtering hanno l'obiettivo di rilevare, monitorare e proteggere le informazioni rilevanti per l'azienda al fine di prevenirne la diffusione non autorizzata anche di natura accidentale. Tali sistemi rilevano quali misure correttive che l'azienda può adottare nell'ambito delle tematiche GDPR e protezione delle informazioni personali e aziendali.

Tali strumenti consentono a livello generale:

- il controllo della fuoriuscita di dati da Pc (ad esempio per copia su sistemi USB o invio su siti Web);
- il controllo della fuoriuscita di dati attraverso strumenti di posta elettronica;
- la verifica della presenza in rete di dati rilevanti non adeguatamente protetti;
- l'identificazione in modo sicuro dei dati rilevanti, tracciandone l'utilizzo e la posizione;
- la regolamentazione dei flussi dei dati rilevanti;
- la protezione di e-mail, supporti rimovibili e singoli file.

L'attività di monitoraggio è eseguita in base a regole che hanno l'obiettivo di identificate tipologie di informazioni specifiche (es. numeri carte di credito, codici fiscali, informazioni anagrafiche e finanziarie) riguardanti dati rilevanti per l'azienda e per i suoi clienti, ed è effettuata con modalità automatiche e semi automatiche. Non sono previsti monitoraggi sistematici su singole utenze. Le notifiche di sicurezza fornite dai sistemi in discorso, saranno sottoposti a specifica analisi tecnica da parte della Funzione di Sicurezza ICT che dovrà stabilire se si tratta di:

- reale anomalia: si procede con l'apertura di un incidente informatico a sistema, avviando il previsto Processo di gestione degli incidenti;
- evento ammesso (falso positivo): l'analisi si ferma e l'utente può continuare con la normale operatività.

Le regole impostate sui sistemi preposti al monitoraggio richiedono un graduale affinamento che con il tempo consente di ridurre il numero delle segnalazioni, migliorando via via la qualità della identificazione di eventuali anomalie.

La Banca ha acquistato ed intende utilizzare uno strumento informatico di Data Loss Prevention fornito da Symantec, leader mondiale nell'ambito della sicurezza dei sistemi e delle informazioni. L'adozione di questo strumento porterà ad una mitigazione del rischio di fuoriuscita dei dati a causa di errori umani o comportamenti non legittimi. Symantec fornisce la soluzione informatica, ma non accede in alcun modo alle informazioni che la stessa gestisce. I dati utilizzati dal sistema di analisi sono di proprietà di Banca Popolare di Sondrio e gestiti e custoditi esclusivamente in strutture del Gruppo collocate all'interno dell'Unione Europea. Ogni variazione sarà tempestivamente comunicata.