VERBALE ACCORDO
DATA LOSS PROTECTION

Siena, 6 novembre 2024

tra Banca MPS SpA
e le Segreterie degli Organi di Coordinamento

Premesso che

- Banca MPS ha dichiarato che in tema di protezione dei dati aziendali, a fronte della necessità di predisporre idonei strumenti di difesa volti a garantire il rigoroso rispetto delle previsioni normative vigenti in coerenza con il General Data Protection Regulation (GDPR), e nell' ottica di mitigare il rischio informatico a cui la Banca è potenzialmente esposta, si rende necessario adottare nuove soluzioni informatiche, finalizzate a tutelare la privacy dei soggetti interessati ed a proteggere i dati rilevanti, che consentano altresì l'individuazione di anomalie di sicurezza non riconoscibili dai sistemi tradizionali oggi utilizzati;

- le predette soluzioni sono quindi finalizzate a minimizzare i rischi relativi alla sicurezza 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 stessi;

- a tal fine il presidio di sicurezza aziendale in materia di Data Loss Prevention (DLP) è stato implementato e integrato con una soluzione informatica di analisi e protezione dei dati aziendali, che consentirà di adeguare i processi interni di controllo;

- il presente accordo integra e sostituisce le previsioni di cui al precedente accordo in materia di Data Loss Protection stipulato tra le Parti il 12 luglio 2022;

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;

- l'Azienda ha dichiarato che l'introduzione della nuova soluzione di Data Loss Prevention adottata è indispensabile per garantire un livello di sicurezza adeguato al rischio derivante dal trattamento dei dati aziendali consentendo di rilevare e prevenire comportamenti anomali e/o di natura sconosciuta da parte di:utenti interni, soggetti e/o attaccanti esterni, che si possono concretizzare in incidenti informatici a vario livello che le soluzioni di sicurezza tradizionali attualmente utilizzate, non sono in grado di rilevare o prevenire;

- l'Azienda 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 complessivo patrimonio aziendale e dei dati personali trattati attraverso metodologie e strumenti integrati ed aggiornati in grado di minimizzare i rischi derivanti dall'utilizzo delle tecnologie informatiche, in aderenza anche alle indicazioni delle Autorità europee in tema di protezione dei dati personali;

- 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 e considerato le Parti
convengono quanto segue:

Art. 1
Le premesse formano parte integrante del presente accordo;

Art. 2
L'Azienda ha dichiarato che la soluzione di Data Loss Prevention adottata consentirà il monitoraggio, con modalità automatiche, dei flussi di dati verso l'esterno dell'azienda finalizzato 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.

Salvo quanto previsto dai successivi articoli, i dati saranno trattati solo per le finalità di sicurezza di cui nelle premesse e per il periodo strettamente necessario a tali scopi (massimo 2 anni), escludendo qualsiasi attività di monitoraggio dellavoratore o gruppi di lavoratori.

Le notifiche di sicurezza fornite dal sistema saranno sottoposte ad analisi da parte delle competenti funzioni di sicurezza logica allo scopo sia di diagnosticare eventuali malfunzionamenti del sistema o falsi positivi sia di verificare l'effettiva presenza di anomalie rispetto ai modelli previsti.

Le analisi effettuate forniranno ulteriore supporto alle consuete e più ampie attività di analisi dei rischi informatici effettuate dalla banca consentendo di migliorare l'efficacia delle misure e dei presidi di sicurezza a tutela del patrimonio informativo aziendale e degli stessi lavoratori.

L'Azienda dichiara che l'utilizzo della soluzione di DLP di cui al presente accordo è aderente alle norme in materia di privacy, ivi compreso 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
La Data Loss Prevention sarà attivata, per dati e documenti classificati come "Confidenziali" e "Strettamente Confidenziali" così come definiti dalla normativa aziendale tempo per tempo vigente, in via progressiva su tutte le strutture della Banca.

Art. 4
Qualora si rendesse necessaria la visualizzazione e l'analisi delle informazioni specifiche di una singola utenza, questa potrà avvenire esclusivamente da parte di personale dipendente appartenente alle funzioni aziendali di controllo oltre che dalle Forze dell'Ordine; la visualizzazione e l'analisi delle informazioni della singola utenza potrà avvenire esclusivamente per le finalità sopra descritte di sicurezza del complessivo patrimonio aziendale e di protezione dei dati, restando pertanto escluso ogni utilizzo delle informazioni ai fini della valutazione delle prestazioni dei dipendenti sotto il profilo sia quantitativo sia qualitativo, nonché a fini disciplinari, fatti salvi i casi di dolo.

Art. 5
Qualora, a seguito delle attività di cui al precedente articolo 4, emergessero elementi di attenzione riconducibili alla attività di un dipendente che possano avere anche rilevanza ai fini disciplinari, le competenti funzioni aziendali forniranno le necessarie comunicazioni al dipendente interessato, che potrà richiedere la visione degli elementi rilevati e farsi assistere da un rappresentante delle organizzazioni sindacali.

Art. 6
Ai fini dell'attuazione dell'adeguata informazione di cui al comma 3 dell'art. 4 legge 300/70, si provvederà all'aggiornamento della normativa D00499 "Regole in materia di tutela dei dati personali", anche alla luce delle eventuali novità normative e si utilizzeranno i consueti canali di comunicazione aziendale.

L'Azienda Le OO.SS