VERBALE DI ACCORDO EX ART. 4 LEGGE 300 DEL 1970

Il giorno 8 maggio 2014, in Bergamo

tra

UNIONE DI BANCHE ITALIANE, nella sua qualità di Capogruppo e dunque anche in nome e per conto delle Banche e Società del Gruppo

e

la Delegazione Sindacale di Gruppo di cui dell'art. 25 dell'Accordo Nazionale in materia di libertà sindacali del 7.7.2010, formata dalle seguenti Organizzazioni Sindacali, rappresentate dalle Segreterie Nazionali, dalle Segreterie degli Organi di Coordinamento e/o dalle Rappresentanze Sindacali Aziendali:

- UNITA' SINDACALE FALCRI SILCEA

Premesso che:

1. il Gruppo ha la necessità di predisporre un presidio di sicurezza del patrimonio informativo e dei programmi presenti nel sistema informatico, allineando il proprio livello di protezione ai più evoluti standard di sistema e contestualmente assicurando il rispetto delle disposizioni tempo per tempo vigenti in materia, mediante l'adeguamento dei sistemi e dei processi aziendali alle prescrizioni emanate dal Garante per la protezione dei dati personali;
2. in attuazione dei principi di cui al precedente punto 1, il Gruppo ritiene di introdurre:
   A. un modello organizzativo e relativi processi in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie in applicazione del Provvedimento del Garante per la protezione dei dati personali n. 192 del 12 maggio 2011;
   B. un'infrastruttura di "mediazione grafica" quale strumento per accedere ai sistemi target sui quali svolgere attività amministrative;
3. la Capogruppo ha illustrato nello specifico alla Delegazione Sindacale il funzionamento dei predetti strumenti di cui intende dotarsi;
4. con particolare riferimento all'argomento di cui al punto 2A e al fine di favorire l'attuazione nelle varie Aziende del citato Provvedimento del Garante per la protezione dei dati personali, ABI e Organizzazioni Sindacali Nazionali hanno sottoscritto l'Accordo Quadro 15.4.2014, che definisce lo "schema generale di accordo" da utilizzare per la stipulazione di intese ex art. 4, comma 2, L. n. 300 del 1970 in specifica attuazione del Provvedimento in oggetto;
5. le Parti Nazionali hanno tra l'altro convenuto nel citato Accordo Quadro che "*ai sensi delle vigenti discipline legislative, ed in particolare della facoltà riconosciuta nell'ambito della contrattazione di secondo livello per la regolazione delle materie inerenti l'organizzazione del lavoro e della produzione, con riferimento, tra l'altro, alla introduzione di nuove tecnologie* (art. 8, commi 1 e 2 del D.L. 13/8/2011 n. 138), *i predetti accordi possono essere stipulati con gli organismi sindacali aziendali di cui all'art. 24 del CCNL 19.1.2012 o, se condiviso tra le parti, con la delegazione di gruppo di cui all'art. 25 dell'Accordo in materia di libertà sindacali del 7.7.2010, considerata la necessaria uniformità ed il carattere eccezionale degli adempimenti connessi all'attuazione del Provvedimento del Garante*";
6. sempre le Parti Nazionali hanno altresì stabilito che "*il confronto a livello aziendale o di gruppo è finalizzato a verificare la coerenza delle proposte dell'impresa con le vigenti disposizioni in materia e con l'Accordo Quadro ed a stipulare i conseguenti accordi ex art. 4, comma 2, L. n. 300 del 1970, entro il mese di aprile 2014, a valere ad ogni conseguente effetto dalla data del 3 giugno 2014*".

Ciò premesso, le Parti convengono quanto segue.

Art. 1

1. La premessa forma parte integrante e sostanziale del presente accordo.

SEZIONE 1

MODELLO ORGANIZZATIVO E RELATIVI PROCESSI IN MATERIA DI CIRCOLAZIONE DELLE INFORMAZIONI IN AMBITO BANCARIO E DI TRACCIAMENTO DELLE OPERAZIONI BANCARIE

Art. 2

Provvedimento del Garante 12.5.2011

1. Le Parti si danno atto in via preliminare che:

a. Il Garante per la protezione dei dati personali ha emanato, in data 12 maggio 2011, il Provvedimento n. 192 avente ad oggetto "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie" e successivamente lo stesso Garante ha emanato, in data 18 luglio 2013, il Provvedimento n. 357 che ne ha differito il termine previsto per l'entrata in vigore;

b. il Provvedimento – che entrerà in vigore il 3 giugno 2014 – è finalizzato a "*garantire il rispetto dei principi in materia di protezione dei dati personali ai sensi del Codice, in ordine ai temi della 'circolazione' delle informazioni riferite ai clienti in ambito bancario e della 'tracciabilità' delle operazioni bancarie effettuate dai dipendenti di istituti di credito*" e detta, ai sensi dell'art. 154, comma 1, lett. c (Codice in materia dei dati personali), prescrizioni in relazione al trattamento di tali dati personali della clientela effettuato dai dipendenti delle "*banche, incluse quelle facenti parte di gruppi,*" delle "*società, anche diverse dalle banche, purché siano parte di tali gruppi*", stabiliti sul territorio nazionale;

c. il Provvedimento riguarda le operazioni relative ai clienti degli istituti bancari di cui al punto che precede, "*sia quelle che comportano movimentazione di denaro, sia quelle di sola consultazione, c.d. inquiry*";

d. il Provvedimento si applica a tutti i lavoratori incaricati dall'azienda dei trattamenti, riconducibili nell'ambito di applicazione del Provvedimento n. 192, come chiarito nel successivo Provvedimento n. 357, quali che siano la qualifica, le competenze, gli ambiti di operatività e le finalità dei trattamenti che sono tenuti a svolgere;

e. il Provvedimento, "*al fine di assicurare il controllo delle attività svolte sui dati dei clienti e dei potenziali clienti da ciascun incaricato del trattamento*", prescrive l'adozione di "*idonee soluzioni informatiche*" per il controllo dei "*trattamenti condotti sui singoli elementi di informazione presenti nei diversi database*"; "*tali soluzioni comprendono la registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari, quando consistono o derivano dall'uso interattivo dei sistemi operato dagli incaricati, sempre che non si tratti di consultazioni di dati in forma aggregata non riconducibili al singolo cliente*";

f. il Provvedimento, in particolare, stabilisce che "*i file di log devono tracciare, per ogni operazioni di accesso ai dati bancari effettuata da un incaricato, almeno le seguenti informazioni:*
   - ✓ *il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso;*
   - ✓ *la data e l'ora di esecuzione;*
   - ✓ *il codice della postazione di lavoro utilizzata;*
   - ✓ *il codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato;*
   - ✓ *la tipologia del rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata*";

g. il Provvedimento prescrive che le predette misure siano adottate "*nel rispetto della vigente disciplina in materia di controllo a distanza dei lavoratori ex art. 4, comma 2, L. 20 maggio 1970, n. 300*";

h. il Provvedimento richiede che siano attivati "*specifici alert*" relativi alle operazioni di inquiry eseguite dagli incaricati volti "*a rilevare intrusioni o accessi anomali ai dati bancari, tali da configurare eventuali trattamenti illeciti*";

Art. 3

Struttura del modello

1. Il Gruppo UBI, ai sensi del Provvedimento del Garante di cui all'articolo 2, adotta un modello organizzativo e relativi processi - nonché connesse soluzioni informatiche - per il controllo dei trattamenti condotti sui singoli elementi di informazione presenti sui diversi database, secondo quanto illustrato e disciplinato dal presente Accordo.

2. Il modello, i processi e il sistema informativo vengono adottati in modo uniforme in tutte le aziende del Gruppo soggette alle disposizioni del Provvedimento del Garante.

3. L'attuazione delle disposizioni del provvedimento del Garante è realizzata mediante prodotti informatici che rappresentano il "Sistema di Gestione delle informazioni e degli eventi di sicurezza (SIEM)". Il SIEM consente l'attivazione di specifici sistemi di monitoraggio (alert) che a loro volta individuano comportamenti potenzialmente anomali o a rischio relativi alle operazioni di inquiry eseguiti dai dipendenti incaricati del trattamento, configurabili come intrusioni o accessi anomali ai dati bancari dei clienti mediante l'utilizzo degli ordinari sistemi informatici aziendali e suscettibili di essere considerati trattamenti illeciti dei dati stessi.

4. Il SIEM garantisce la riservatezza e inalterabilità delle informazioni secondo i più moderni standard riconosciuti.

Art. 4

Sistema di tracciamento

1. Le varie funzioni del sistema informativo vengono modificate al fine di consentire la "*registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie* (esclusivamente di interrogazione) *effettuate sui dati bancari*" da tutti gli incaricati del trattamento.

2. In particolare, il sistema prevede, in modo automatico:

   2.1. la cattura e l'archiviazione su un'apposita struttura (staging area) dei seguenti dati, previsti dal Provvedimento del Garante:

      2.1.1. matricola (codice identificativo) dell'operatore
      2.1.2. data/ora dell'evento
      2.1.3. postazione di lavoro
      2.1.4. codice NDG del cliente interrogato
      2.1.5. rapporto oggetto di interrogazione o identificativo del cliente da cui lo stesso possa essere dedotto

   2.2. il controllo di validità dei predetti dati e il loro arricchimento, più volte al giorno e sempre all'interno della staging area, con le seguenti ulteriori informazioni, necessarie per la generazione degli alert:

      2.2.1. informazioni acquisite da altri sistemi aziendali:
         - ✓ con riferimento al dipendente che ha eseguito l'interrogazione: funzione utilizzata, mansione e unità operativa
         - ✓ con riferimento al cliente oggetto dell'interrogazione: unità operativa e tipo di mercato;

      2.2.2. informazioni calcolate dal sistema stesso, sulla base di apposite tabelle previste nel sistema di alert: tipologia di unità operativa, fascia di orario di accesso ai dati, secondo quanto meglio precisato nel successivo articolo 5.

3. Successivamente alle fase sopra descritte, tutte le informazioni raccolte ("*log di tracciamento delle operazioni di inquiry*") vengono automaticamente trasferite dalla staging area - dalla quale vengono contestualmente e automaticamente cancellate - al SIEM e qui conservate per un periodo di 24 mesi, fatte salve esigenze di forza maggiore. Oltre tale limite temporale la conservazione è ammessa esclusivamente in presenza di specifici vincoli di legge in materia.

Art. 5

Sistema di alert

1. Come specificamente richiesto dal Garante, sono attivati in automatico dal SIEM "*specifici alert*" finalizzati ad individuare "*comportamenti anomali o a rischio*", rilevati dal SIEM stesso in funzione degli indicatori sopra individuati al punto 2.2.2, ossia:

   1.1. fascia oraria in cui è stata eseguita l'operazione (giorni lavorativi o non lavorativi, orario d'ufficio o extra)

   1.2. macro-struttura organizzativa di appartenenza del dipendente e di riferimento del cliente (strutture centrali, di supporto alla rete o di rete).

2. Il SIEM effettua propri automatici controlli sui dati di cui all'articolo 4, elaborati in funzione dei parametri di cui al precedente comma 1, generando una segnalazione di anomalia (alert) nel caso in cui vengano superate specifiche soglie di monitoraggio, identificate con un numero predeterminato dall'azienda, oltre il quale gli accessi sono presunti come anomali.

Art. 6

Controlli

1. L'attività di controllo degli alert è demandata, ai sensi del Provvedimento del Garante, "*a unità organizzativa o, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti*".

2. In particolare viene identificata per tutto il Gruppo la struttura di Risorse Umane di ciascuna Azienda quale unità preposta a ricevere le segnalazioni del SIEM di cui al comma 2 del precedente articolo e ad effettuare - esclusivamente su queste segnalazioni, oltre ai casi di controlli a campione previsti dal Provvedimento - le verifiche di volta in volta necessarie. In ogni caso, resta escluso che le informazioni in esame vengano utilizzate a fini gestionali delle risorse.

3. Ove siano ravvisati elementi dai quali sia possibile desumere una eventuale anomalia, la struttura di Risorse Umane coinvolge nell'analisi della segnalazione e per le conseguenti rispettive verifiche, le seguenti ulteriori strutture, in successione:

   1.1. il Responsabile aziendale del trattamento dei dati dei dipendenti

   1.2. il Direttore Generale dell'Azienda

   1.3. la struttura di Audit.

4. Qualora, nel corso delle analisi di cui sopra, dovessero emergere profili di particolare gravità, verrà inviata una comunicazione al Dipendente interessato, con l'indicazione della verifica in corso. In tal caso, il dipendente potrà essere sentito, anche su sua richiesta, con l'assistenza di un rappresentante sindacale dell'Organizzazione a cui aderisce o conferisce mandato.

5. Ai sensi del Provvedimento del Garante "*la gestione dei dati bancari deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti*".

6. Le Parti si danno atto che, sempre ai sensi del Provvedimento, "*i controlli devono comprendere anche verifiche a posteriori, a campione o a seguito di allarme derivante da sistemi di alerting e di anomaly detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte altresì verifiche periodiche sulla corretta conservazione dei file di log per il periodo*" sopra previsto (articolo 4, comma 3).

7. Come previsto dal Provvedimento, "*l'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate*".

****

8. In considerazione della particolare attività di cui al comma 2 del presente articolo, verranno assoggettati a tracciamento anche gli accessi al SIEM, indispensabili per svolgere le anzidette attività, degli incaricati delle varie strutture di Risorse Umane, nonché altri eventuali accessi al SIEM stesso degli incaricati all'amministrazione del sistema (dipendenti Ubiss specificamente individuati), necessari per la manutenzione dell'impianto.

SEZIONE 2

INFRASTRUTTURA DI "MEDIAZIONE GRAFICA" QUALE STRUMENTO PER ACCEDERE AI SISTEMI TARGET

Art. 7

Patrimonio informativo e dei programmi presenti nel sistema informatico aziendale
Presidio di sicurezza

1. Le Parti si danno atto in via preliminare che:

a. il Gruppo, come già evidenziato nelle premesse al presente accordo, ha la necessità di predisporre un evoluto ed adeguato presidio di sicurezza del patrimonio informativo e dei programmi presenti nel sistema informatico;

b. anche il Garante per la protezione dei dati personali, con vari provvedimenti succedutisi nel tempo (Provvedimento del 27.11.2008 e del 25.6.2009), ha richiamato i Titolari del trattamento dei dati stessi in merito all'esigenza di valutare con particolare attenzione l'attribuzione al Personale di funzioni tecniche corrispondenti o assimilabili a quelle di Amministratore di Sistema (Amministratore di base di dati o Amministratore di rete) laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali;

c. in particolare il Garante ha stabilito che debbano essere "*adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di Sistema. Le registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la registrazione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a 6 mesi*";

d. a tal fine il Gruppo ha comunicato alle Organizzazioni Sindacali la volontà di introdurre presso UBISS lo strumento denominato "Mediatore Grafico", che permette agli operatori IT interni ed esterni della stessa UBIS di accedere ai sistemi target su cui devono svolgere le proprie attività amministrative; tale infrastruttura consente agli utenti di accedere da remoto ai sistemi target di cui si compone il sistema informatico (rete, server, applicazioni, database ecc.) attraverso metodologie semplici e snelle quali Browser web, remote desktop e sessioni a riga di comando;

e. tale strumento, tra l'altro, consente di tracciare gli accessi (login e logout secondo i requisiti stabiliti dal Garante), i comandi lanciati e le attività eseguite, registrandone i relativi fotogrammi con la sequenza operativa della singola attività svolta dall'operatore per l'esecuzione dell'intervento operativo (i fotogrammi riproducono tutte le variazioni avvenute sullo schermo dell'operatore sia per le fasi di input sia per le fasi di output);

Art. 8

Oggetto della registrazione

1. L'utilizzo del Mediatore Grafico consente la registrazione e l'analisi di tutte le tipologie di accesso ai sistemi di rete, ai sistemi di sicurezza e ai sistemi Server comprensivi di database. In particolare si tratta dei cd. "*accessi da remoto*" ovvero gli accessi ai sistemi aziendali da parte degli amministratori di sistema che avvengono tramite postazioni aziendali di UBI Sistemi e Servizi oppure al di fuori dei locali della Società (come ad esempio nel caso di interventi in reperibilità).

2. Con riferimento invece agli "*accessi in locale*" - ovvero l'accesso ai sistemi aziendali che avviene direttamente sui sistemi aziendali e che non viene veicolato dai sistemi di 'Mediazione' - l'operatività degli amministratori di sistema verrà registrata attraverso un software installato sul sistema oggetto di manutenzione/utilizzo.

Art. 9

Finalità

1. L'utilizzo dello strumento descritto, nel rispetto delle normative vigenti in materia, ha lo scopo di garantire la sicurezza dei dati presenti nel sistema informatico aziendale da un eventuale trattamento

non conforme alle normative e alle disposizioni aziendali, nonché di tutelare i soggetti terzi, ai quali i dati si riferiscono, da possibili trattamenti non idonei o vietati.

Art. 10

Conservazione delle immagini

1. I tempi di conservazione delle immagini sono quelli stabiliti dalle normative tempo per tempo vigenti in materia, con specifico riferimento alle disposizioni aziendali, nonché alle indicazioni contenute nei Provvedimenti del Garante già citati in premessa (attualmente la conservazione è prevista per 2 anni).

2. I fotogrammi vengono salvati e archiviati su supporti informatici (nastri) e cancellati automaticamente alla scadenza.

Art. 11

Ricerca e visualizzazione delle immagini registrate

1. L'accesso ai supporti informatici di cui al precedente articolo 10 è consentito solo a personale UBIS della Direzione Operations formalmente individuato e incaricato della visualizzazione degli stessi dalle disposizioni aziendali in materia, anche sulla base di specifiche indicazioni da parte di funzioni di controllo di Capogruppo, nell'ambito delle necessità collegate all'attività di presidio della sicurezza del sistema Informativo, nonché per esigenze tecniche di UBIS collegate a successivi accessi e interventi sul medesimo database.

2. Nel rispetto delle condizioni di cui sopra, gli accessi ai sistemi di ricerca e visualizzazione delle immagini avvengono in ottemperanza alla normativa vigente e mediante l'utilizzo di profili di accesso specifici e personali.

3. La Direzione Operations di UBIS informerà tempestivamente (ove possibile preventivamente) la Direzione Risorse Umane della stessa UBIS degli accessi alle registrazioni; quest'ultima, per il tramite delle competenti strutture della Capogruppo, provvederà a fornire la relativa comunicazione alle Parti Sindacali di Gruppo firmatarie del presente accordo.

4. Nei casi di cui al comma che precede, le immagini registrate potranno essere visionate, entro 3 giorni di calendario dalla comunicazione, anche da uno dei rappresentanti sindacali della Organizzazione, firmataria del presente accordo, a cui il dipendente interessato risulti iscritto o conferisca mandato. Nel caso di dipendente non iscritto, le immagini registrate potranno essere visionate da uno dei rappresentanti sindacali delle Sigle che hanno sottoscritto il presente verbale (secondo la logica della rotazione tra le Sigle firmatarie, seguendo l'ordine alfabetico), entro il medesimo termine di cui sopra.

SEZIONE 3

DISPOSIZIONI FINALI

Art. 12

Informativa al Personale

1. Il Personale viene informato delle procedure adottate ai sensi delle precedenti sezioni 1 e 2 e dei connessi adempimenti tramite le consuete modalità di informativa aziendale, che viene portata a conoscenza di tutti i lavoratori interessati. Inoltre, nell'ambito di quanto previsto dall'art. 72 del CCNL 19.1.2012, possono svolgersi, ove necessario, specifiche attività formative retribuite.

2. In particolare, sarà resa disponibile entro il 30 settembre 2014 apposita formazione a distanza rivolta a tutto il Personale. Potranno essere previste, anche nell'ambito di corsi di formazione in aula già disponibili/programmati, ulteriori specifici interventi sulla materia oggetto del presente accordo, anche sulla base delle effettive necessità rilevate negli incontri di verifica di cui al successivo articolo 13.

Art. 13

Incontri di verifica

1. A richiesta di una delle Parti si darà luogo ad incontri di verifica annuali a livello di Gruppo in merito all'applicazione delle disposizioni contenute nel presente Accordo. Per l'anno 2014 il primo incontro tra le Parti sarà convocato entro il 15 ottobre per la verifica congiunta della funzionalità del sistema in sede di prima applicazione e per le valutazioni relative ad eventuali affinamenti.

2. Inoltre, il Gruppo fornirà periodicamente (ogni sei mesi) dati in forma aggregata per azienda circa la quantità e la qualità degli alert di cui alla sezione 1, degli accessi di cui alla sezione 2 e degli altri controlli a campione, emersi nel periodo di riferimento. Specifica informazione verrà tempestivamente fornita nei casi di cui al comma 4 dell'articolo 6.

3. Viene comunque prevista la necessità di un incontro preventivo nel caso in cui il Gruppo introduca significative variazioni agli strumenti di cui al presente Accordo. Nel corso di tale incontro le Parti valuteranno congiuntamente la conseguente eventuale necessità di integrare il presente Accordo.

Art. 14

Disposizioni finali

1. L'utilizzo degli strumenti regolati dal presente Accordo è finalizzato esclusivamente ad adempiere alle necessità illustrate in premessa, con particolare riferimento agli adempimenti previsti dai Provvedimenti del Garante citati nell'Accordo stesso. Viene pertanto esclusa ogni altra finalità, diretta o indiretta, di controllo a distanza dei Dipendenti, escludendo altresì espressamente che l'uso dei dati o la visualizzazione di immagini possa avvenire per scopi relativi alla sfera soggettiva del Dipendente interessato.

2. Per quanto non espressamente richiamato nel presente Accordo, si fa rinvio alle correlate prescrizioni dell'Accordo Quadro Nazionale 15.4.2014 e del Provvedimento del Garante per la protezione dei dati personali.

3. Il presente verbale è sottoscritto con la delegazione di gruppo di cui all'art. 25 dell'Accordo in materia di libertà sindacali del 7.7.2010, ai sensi dell'art. 8, commi 1 e 2 del D.L. 13/8/2011, n. 138.

Letto, confermato e sottoscritto.

UBI Banca S.c.p.a.

UNITA' SINDACALE FALCRI SILCEA