VERBALE DI ACCORDO

Il giorno 29 settembre 2014, in Modena,

tra

l'Azienda Banca popolare dell'Emilia Romagna – Soc. Coop. in veste di azienda Capogruppo (di seguito, per brevità, "BPER") e in nome e per conto delle aziende coinvolte, nelle persone dei Sigg. Giuseppe Corni, Stefano Verdi, Andrea Prandi, Corrado Odorici, Roberto Testoni, Federica Tognacci e Marcello Bongiorni

e le Delegazioni di Gruppo delle Organizzazioni Sindacali:
DIRCREDITO
FABI
FIBA/CISL
FISAC/CGIL
SINFUB
UILCA

premesso che:

- il d.lgs. 30 giugno 2003, n. 196, rubricato "Codice in materia di protezione dei dati personali" stabilisce che chiunque ha diritto alla protezione dei dati personali che lo riguardano e disciplina, tra l'altro, compiti e funzioni del Garante per la protezione dei dati personali;
- il Garante per la protezione dei dati personali, ha il compito di prescrivere, anche d'ufficio, ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento dei dati conforme alle disposizioni vigenti;
- 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"; in data 18 luglio 2013, lo stesso Garante ha emanato il Provvedimento n. 357 e ne ha differito il termine previsto per l'entrata in vigore;
- in data 22 maggio 2014, lo stesso Garante ha emanato il Provvedimento n. 257 e ne ha prorogato il termine per l'entrata in vigore;
- il Provvedimento – che entra in vigore, a seguito della predetta proroga, il 30 settembre 2014 – è finalizzato a "garantire il rispetto dei principi in materia di protezione dei dati personali ai sensi del relativo Codice, in ordine ai temi della «circolazione» delle informazioni riferite ai clienti in ambito bancario e della «tracciabilità» delle operazioni bancarie" e detta prescrizioni, ai sensi dell'art. 154, comma 1, lett. c), 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;
- 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*";
- 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";
- 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";

- in data 15 aprile 2014 è stato sottoscritto tra ABI e le OO.SS. l'accordo quadro nazionale sull'applicazione del Provvedimento del Garante per la protezione dei dati personali del 12 maggio 2011, n. 192, che qui si dà per integralmente trascritto e che definisce lo schema generale di accordo da utilizzare per la sottoscrizione di intese ex art. 4, comma 2, L. n. 300/1970 in specifica attuazione del Provvedimento in oggetto;
- tale accordo quadro stabilisce tra l'altro 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, i predetti accordi possono essere stipulati con gli organismi sindacali aziendali di cui all'art. 24 del ccnl 19 gennaio 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 luglio 2010, considerata la necessaria uniformità ed il carattere eccezionale degli adempimenti connessi all'attuazione del Provvedimento del Garante"*;
- nella medesima intesa di cui al precedente alinea le Parti hanno convenuto 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 ed il presente 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 per i soli effetti connessi all'applicazione del Provvedimento;*
- la Capogruppo, in occasione degli incontri sindacali del 3 e 26 giugno scorsi ha illustrato alla Delegazione di Gruppo delle OO.SS. le logiche ed i criteri dell'applicativo informatico utilizzato per adempiere alle prescrizioni del Provvedimento del Garante; avviando il confronto a livello di Gruppo finalizzato a verificare la coerenza delle proposte dell'impresa con le vigenti disposizioni in materia di cui alle premesse e finalizzato a stipulare i conseguenti accordi ex art. 4, comma 2, l. n. 300 del 1970;
- in occasione dei suddetti incontri, parte aziendale ha consegnato ed illustrato alle OO.SS. la propria proposta di verbale di accordo corredata delle relative schede tecniche esplicative dello svolgimento di tale attività;
- rispetto al citato verbale, le OO.SS. hanno evidenziato la necessità di approfondire ulteriormente gli aspetti legati ai parametri utilizzati per la generazione degli alert, proponendo all'azienda di effettuare un periodo di sperimentazione ed analisi;
- lo scorso 7 agosto le Parti hanno sottoscritto un'intesa, volta a disciplinare l'effettuazione di una fase sperimentale finalizzata alla sottoscrizione dell'intesa ex art. 4, comma 2, L. n. 300/1970 in specifica attuazione del Provvedimento in oggetto;
- in data odierna l'Azienda ha illustrato alla Delegazione di Gruppo delle OO.SS. gli esiti della suddetta fase sperimentale, evidenziando l'opportunità di proseguire nell'attività di *"fine tuning"* della procedura anche successivamente all'entrata in vigore del Provvedimento, data da cui decorrerà la messa in funzione della stessa; l'Azienda si è altresì resa disponibile, in questa prima fase di avvio e fino alla completa messa a regime del sistema, ad incontrare periodicamente la Delegazione di Gruppo delle OO.SS. per confrontarsi con le stesse in merito al funzionamento della procedura;
- in applicazione di quanto precede, Banca popolare dell'Emilia Romagna in qualità di Capogruppo e le Delegazioni Sindacali di Gruppo intendono sottoscrivere il presente accordo, che definisce i principi e linee guida valevoli per tutte le società del gruppo rientranti nell'ambito di applicazione del Provvedimento del Garante per la protezione dei dati personali del 12 maggio 2011, n. 192;

si conviene quanto segue:

Art. 1

La premessa costituisce parte integrante e sostanziale del presente verbale di accordo che:

- si applica a tutte le Banche e Società del Gruppo Banca popolare dell'Emilia Romagna elencate nell'allegato n. 1 al presente accordo;

- conferma che le soluzioni informatiche presentate sono destinate esclusivamente al controllo dei trattamenti condotti sui singoli elementi di informazione presenti sui diversi database, ai sensi di quanto prescritto dal Garante per la protezione dei dati personali con il Provvedimento n. 192 del 12 maggio 2011.

Art. 2

I sistemi informativi sono impostati ai fini della registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari da tutti gli incaricati del trattamento.

In particolare, come previsto dall'art. 9 dell'accordo quadro citato in premessa, i file di log tracceranno, per ogni operazione di accesso ai dati bancari effettuata da un incaricato, 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 di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata.

Art. 3

I log di tracciamento delle operazione di inquiry saranno conservati per un periodo di 24 mesi dalla data di registrazione dell'operazione, fatte salve esigenze di forza maggiore. Oltre tale limite temporale la conservazione è ammessa in presenza di specifici vincoli di legge in materia.

Art. 4

Le specifiche tecniche e organizzative apprestate, riportate negli allegati n. 2, 3, 4, sono state illustrate e discusse con la Delegazione di Gruppo nel corso del confronto e formano parte integrante del presente accordo.

Le eventuali future modifiche, se significative, formeranno oggetto di specifica informativa alla Delegazione Sindacale di Gruppo nel corso di un apposito incontro, nell'ambito del quale le parti valuteranno se modificare o integrare l'accordo stesso; successivamente saranno oggetto di illustrazione in sede aziendale.

Art. 5

Come espressamente richiesto dal Garante, sono attivati specifici alert finalizzati ad individuare comportamenti anomali o a rischio relativi alle operazione di inquiry eseguite dagli incaricati del trattamento, come specificato più in dettaglio negli allegati alla presente intesa.

Art. 6

Ai sensi del Provvedimento n. 192 del 12 maggio 2011 e successive integrazioni:

- la gestione dei dati bancari è oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento[1], 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;
- l'attività di controllo è demandata ad una unità organizzativa (vedi allegati) o, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti;
- i controlli comprendono anche verifiche a posteriori, a campione o a seguito di allarme derivante da sistemi 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;

[1] Cfr. artt. 4[1f] e 28 D.Lgs. 196/2003

- l'attività di controllo è 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.

Art. 7
I lavoratori incaricati sono informati delle procedure adottate e dei connessi adempimenti tramite apposita informativa (art. 13 d.lgs. n. 196 del 2003), che deve essere portata a conoscenza di tutti i lavoratori attraverso specifici ed opportuni strumenti. Inoltre, nell'ambito di quanto previsto dall'art. 72 del Ccnl 19 gennaio 2012, possono svolgersi, ove necessario, specifiche attività formative retribuite.

Art. 8
L'uso degli strumenti disciplinati dal presente verbale di accordo, in coerenza con gli obiettivi del Provvedimento, è finalizzato esclusivamente a dar corso agli adempimenti previsti dai citati Provvedimenti del Garante, restando pertanto esclusa qualsiasi finalità di controllo a distanza dei dipendenti, nel rispetto di quanto previsto dall'articolo 4 della L. 300/70.

Art. 9
In sede aziendale saranno effettuati incontri di verifica annuale in merito all'applicazione degli accordi in materia con riferimento al numero e alla qualità di alert generati.
Il primo incontro si terrà entro il 31/1/2015.

Art. 10
Agli Organismi Sindacali firmatari del presente verbale verranno fornite informazioni in ordine alla/e unità organizzativa/e cui tempo per tempo sarà affidato il trattamento dei dati bancari dei clienti in base a quanto previsto dal Provvedimento oggetto del presente accordo, nonché sulle modalità di indagine a campione.

Art. 11
Per quanto altro non espressamente richiamato nel presente verbale di accordo, si fa rinvio alle correlate prescrizioni dell'Accordo Quadro Nazionale del 15 aprile 2014 e del Provvedimento del Garante per la protezione dei dati personali della clientela.

Le Organizzazioni Sindacali:

DIRCREDITO – F.D.
FABI
FIBA-CISL
FISAC-CGIL
SINFUB
UIL.CA

BANCA POPOLARE DELL'EMILIA ROMAGNA
Società Cooperativa

Allegato 1 – Elenco Banche e Società

- BANCA POPOLARE DELL'EMILIA ROMAGNA
- BANCO DI SARDEGNA
- BANCA DELLA CAMPANIA
- BANCA POPOLARE DEL MEZZOGIORNO
- BANCA POPOLARE DI RAVENNA
- BANCA DI SASSARI
- BPER SERVICES
- OPTIMA
- BPER TRUST COMPANY
- NETTUNO GESTIONE CREDITI

- CASSA DI RISPARMIO DI BRA - Allegato n. 3
- SARDALEASING - Allegato n. 4

Scheda esplicativa dati tecnici
Allegato n.2 – accordo 29 settembre 2014

Caratteristiche tecniche: Base dati host, collocata in infrastruttura standard. Previsti salvataggi di backup secondo i processi standard.
Ubicazione: server farm Bperservices.
Termine di conservazione : come previsto dall'articolo 3 del presente accordo.
Modalità di accesso: Con riconoscimento ruoli e profili sistemistici secondo processi standard.

Dettagli tecnici log e flussi:
Caratteristiche tecniche: Flussi di dati dipartimentali e host, spediti e ricevuti mediante processi e strumenti di trasferimento file standard.
Ubicazione: server farm Bperservices.
Termine di conservazione: come previsto dall'articolo 3 del presente accordo.
Modalità di accesso: con riconoscimento ruoli e profili sistemistici secondo processi standard.

Come richiesto dal provvedimento emesso dal Garante per la protezione dei dati personali, verranno tracciate tutte le operazioni bancarie che trattino dati di clienti soggetti alla normativa privacy vigente (persone fisiche come classificate in anagrafe di gruppo).

Le informazioni da tracciare sono registrate dalle singole procedure informatiche sulla base dati host centralizzata e sono:

a) il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso (matricola di chi ha eseguito l'operazione);
b) la data e l'ora di esecuzione;
c) il terminale della postazione di lavoro utilizzata e l'identificativo ufficio dal quale è avvenuta (filiale/ufficio/sezione);
d) l'identificativo del cliente interessato dall'operazione di accesso ai dati bancari o l'identificativo del rapporto interessato dall'operazione di accesso;
e) la tipologia di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata.

Gli ulteriori dati memorizzati sulla base dati host centralizzata sono:

f) il codice della banca/società in cui è eseguita l'operazione;
g) ulteriori dati atti ad identificare la tipologia di transazione utilizzata ed il tracciato informatico usato (codice procedura);
h) ulteriori dati descrittivi atti ad identificare l'operazione posta in essere, valorizzati da ciascun servizio alimentante (codice transazione).

Tali informazioni vengono inviate giornalmente tramite un file transfer automatico ad una base dati dipartimentale che raccoglie le informazioni per i tempi di conservazione previsti all'art. 3 del presente accordo. Tutta l'attività di estrazione , invio e ricezione è automatizzata.

Le strutture tecnologiche utilizzate sono standard e di mercato.

Durante il passaggio dei dati dall'infrastruttura host all'infrastruttura dipartimentale atta a generare gli alert previsti dal provvedimento i tracciati vengono transcodificati attraverso i seguenti dati :

- nome/cognome e codice fiscale dell'operatore che ha posto in essere l'operazione;
- l'eventuale codice azienda di distacco dell'operatore che ha posto in essere l'operazione;
- il codice filiale/ufficio/sezione di appartenenza del soggetto che ha posto in essere l'operazione;
- l'informazione se la posizione interrogata appartenga o meno ad un dipendente;
- ulteriori informazioni sulla posizione interrogata nei casi in cui siano reperibili dal sistema informativo di gruppo (codice fiscale del soggetto interessato dall'operazione/codice ndg/estremi del rapporto/stato di cointestato o meno);
- ulteriori dati descrittivi atti ad aiutare l'attività di generazione ed analisi degli alert (la descrizione della filiale/ufficio di appartenenza, la descrizione della filiale operante, la descrizione della transazione utilizzata, le mansioni dell'operatore divise tra filiale ed ufficio centrale).

Sulla base dati dipartimentale è prevista la creazione di alert giornalieri atti ad evidenziare le situazioni di attenzione.

Sistema degli *alert*

Attraverso strumenti di *business intelligence* all'uopo parametrizzati, come previsto dal provvedimento del Garante, sono impostati *alert* finalizzati a segnalare eventuali situazioni anomale emerse principalmente a seguito dell'analisi di:

1) fasce orarie di operatività (compresi orari, giorni non lavorativi e/o assenze);
2) accessi su rapporti non radicati o non gestiti presso/dalla struttura di appartenenza del dipendente;
3) ruolo dell'operatore;

L'alert è generato automaticamente quando tali parametri e/o una combinazione di essi superano una soglia prestabilita rispetto frequenze e livelli di riferimento definiti ad una normale operatività. Nel rispetto del principio della segregazione dei compiti previsti dalla normativa, i profili autorizzativi ed i diritti di accesso ai dati bancari sono adeguatamente gestiti e controllati, di conseguenza non possono verificarsi transazioni al di fuori dei ruoli organizzativi autorizzati.

L'accesso alle informazioni obbligatoriamente archiviate ed all'applicativo di generazione degli alert sarà consentito al Servizio Compliance di Gruppo - Ufficio Normative Trasversali - Sezione Presidio Privacy, all'Ufficio Gestione Normativa di Gruppo del Servizio Presidio Organizzativo di Gruppo e Normativa e, con competenza sul Banco di Sardegna e Banca di Sassari, all'Ufficio Normativa e Amministrazione costituito presso il Banco di Sardegna, nonché alle funzioni aziendali di controllo ed ai gestori informatici dell'applicativo competenti secondo ruoli e responsabilità". Eventuali modifiche nella struttura organizzativa della Capogruppo, anche a seguito del completamento delle programmate fusioni, potranno comportare modifiche alle denominazioni e/o al perimetro delle unità organizzative che accedono alle informazioni in parola: di tali modifiche si darà opportuna informativa.

In caso di generazione automatica di alert, le Strutture aziendali incaricate del presidio continuativo delle informazioni, qualora dovessero rilevare profili anomali, potranno segnalare alle funzioni aziendali di controllo ed alla Direzione Risorse Umane di Gruppo le situazioni di potenziale violazione della privacy e senza ritardo il dipendente verrà informato, senza che ciò costituisca avvio di procedura disciplinare ai sensi dell'art. 7 Legge 300, in merito alla verifica in corso e potrà essere sentito, anche su sua richiesta, con l'eventuale assistenza di un rappresentante sindacale dell'Organizzazione cui aderisce o conferisce mandato.

Gli accessi eseguiti da tali strutture sono a loro volta tracciati e conservati per i tempi di conservazione previsti all'art. 3 del presente accordo.

Allegato n. 3 - accordo 29 settembre 2014
Scheda esplicativa dati tecnici e descrizione processo di gestione degli alert CR Bra

Caratteristiche tecniche: Base dati host, collocata in infrastruttura standard. Previsti salvataggi di backup secondo i processi standard.
Ubicazione: server farm SBA (Servizi Bancari Associati – Cuneo. Out-sourcer del sistema informativo).
Termine di conservazione: come previsto dall'articolo 3 del presente accordo.
Modalità di accesso: Con riconoscimento ruoli e profili sistemistici secondo processi standard.

Dettagli tecnici log e flussi:
Caratteristiche tecniche: Flussi di dati dipartimentali e host, spediti e ricevuti mediante processi e strumenti di trasferimento file standard.
Ubicazione: server farm SBA (Servizi Bancari Associati – Cuneo. Out-sourcer del sistema informativo).
Termine di conservazione: come previsto dall'articolo 3 del presente accordo.
Modalità di accesso: Con riconoscimento ruoli e profili sistemistici secondo processi standard.

Come richiesto dal provvedimento emesso dal Garante per la protezione dei dati personali, verranno tracciate tutte le operazioni bancarie che trattino dati di clienti soggetti alla normativa privacy vigente (persone fisiche come classificate in anagrafe procedurale CR Bra).

Le informazioni da tracciare sono registrate dalle singole procedure informatiche sulla base dati host centralizzata e sono:

a) il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso (matricola di chi ha eseguito l'operazione);
b) la data e l'ora di esecuzione;
c) il terminale della postazione di lavoro utilizzata e l'identificativo ufficio dal quale è avvenuta (filiale/ufficio/sezione);
d) l'identificativo del cliente interessato dall'operazione di accesso ai dati bancari o l'identificativo del rapporto interessato dall'operazione di accesso;
e) la tipologia di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata.

Gli ulteriori dati memorizzati sulla base dati host centralizzata sono:

f) il codice della banca in cui è eseguita l'operazione;
g) ulteriori dati atti ad identificare la tipologia di transazione utilizzata ed il tracciato informatico usato (codice procedura);
h) ulteriori dati descrittivi atti ad identificare l'operazione posta in essere, valorizzati da ciascun servizio alimentante (codice transazione).

Tali informazioni vengono inviate giornalmente tramite un file transfer automatico ad una base dati dipartimentale che raccoglie le informazioni per i 24 mesi previsti dal provvedimento.
Tutta l'attività di estrazione, invio e ricezione è automatizzata.

Le strutture tecnologiche utilizzate sono standard e di mercato.

Sulla base dati dipartimentale è prevista la creazione di alert settimanali atti ad evidenziare le situazioni di attenzione.

Sistema degli *alert*

Attraverso strumenti di *business intelligence* all'uopo parametrizzati, come previsto dal provvedimento del Garante, sono impostati *alert* finalizzati a segnalare eventuali situazioni anomale emerse principalmente a seguito dell'analisi di:

1) fasce orarie di operatività (compresi orari, giorni non lavorativi e/o assenze);
2) accessi su rapporti non radicati o non gestiti presso/dalla struttura di appartenenza del dipendente;
3) ruolo dell'operatore;

L'alert è generato automaticamente quando tali parametri e/o una combinazione di essi superano una soglia prestabilita rispetto frequenze e livelli di riferimento definiti ad una normale operatività. Nel rispetto del principio della segregazione dei compiti previsti dalla normativa, i profili autorizzativi ed i diritti di accesso ai dati bancari sono adeguatamente gestiti e controllati, di conseguenza non possono verificarsi transazioni al di fuori dei ruoli organizzativi autorizzati.

L'accesso alle informazioni obbligatoriamente archiviate ed all'applicativo di generazione degli alert sarà consentito all'Ufficio Organizzazione e Servizi – Cost Management ed ai Referenti Compliance, nonché alle funzioni aziendali di controllo ed ai gestori informatici dell'applicativo competenti secondo ruoli e responsabilità". Eventuali modifiche nella struttura organizzativa della CR Bra, potranno comportare modifiche alle denominazioni e/o al perimetro delle unità organizzative che accedono alle informazioni in parola: di tali modifiche si darà opportuna informativa.

In caso di generazione automatica di alert, le Strutture aziendali incaricate del presidio continuativo delle informazioni, qualora dovessero rilevare profili anomali, potranno segnalare alle funzioni aziendali di controllo ed alla Direzione Risorse Umane di Gruppo le situazioni di potenziale violazione della privacy e senza ritardo il dipendente verrà informato, senza che ciò costituisca avvio di procedura disciplinare ai sensi dell'art. 7 Legge 300, in merito alla verifica in corso e potrà essere sentito, anche su sua richiesta, con l'eventuale assistenza di un rappresentante sindacale dell'Organizzazione cui aderisce o conferisce mandato.

Gli accessi eseguiti da tali strutture sono a loro volta tracciati e conservati per i tempi di conservazione previsti all'art. 3 del presente accordo.

Allegato n. 4 accordo 29 settembre 2014
Scheda esplicativa dati tecnici e descrizione processo di gestione degli alert Sardaleasing

Caratteristiche tecniche: Base dati host, collocata in infrastruttura aziendale su applicativo e modulo LOGOS (LEASINGMOD 400, e-LEASINGMOD, CREDEL).
Previsti salvataggi di backup secondo i processi standard.
Ubicazione: server farm Bpservices.
Termine di conservazione: come previsto dall'articolo 3 del presente accordo.
Modalità di accesso: Con riconoscimento matricola e profili sistemistici, secondo modalità standard.

Dettagli tecnici log e flussi:
Caratteristiche tecniche: Flussi di dati dipartimentali
Ubicazione: Società, Data Base aziendale
Termine di conservazione: come previsto dall'articolo 3 del presente accordo.
Modalità di accesso: Con riconoscimento matricola e profili sistemistici secondo modalità standard.

Come richiesto dal provvedimento emesso dal Garante per la protezione dei dati personali, verranno tracciate tutte le operazioni che trattino dati di clienti.

Le informazioni da tracciare sono registrate sulla base dati centralizzata (LOGOS) e sono:
- codice identificativo utente accedente;
- data e ora di accesso;
- codice postazione utente accedente;
- nome e numero del lavoro (job name) attribuito dalla macchina;
- nome e breve descrizione del programma richiamato;
- codice controparte interrogata;
- filiale ed area utente interrogante;
- filiale ed area controparte interrogata.

Tali informazioni vengono giornalmente salvate su una base dati che raccoglie le informazioni per i 24 mesi previsti dal provvedimento.
Tutta l'attività di estrazione, invio e ricezione è automatizzata.

Le strutture tecnologiche utilizzate sono standard e di mercato (Fornitore Logos SRL, Brescia)
Sulla base dati è prevista la creazione di alert giornalieri atti ad evidenziare le situazioni di attenzione.

Per la generazione degli alert previsti dal provvedimento i tracciati vengono transcodificati con i seguenti dati:
- nome/cognome/ragione sociale controparte interrogata;
- forma giuridica della controparte interrogata;
- tipo rapporto controparte interrogata:
  - o cliente;
  - o fornitore;
  - o brokers;

o garanti/fidejussori;
o coobbligati;
o dealers.

Sistema degli *alert*

Attraverso strumenti di *business intelligence* all'uopo parametrizzati, come previsto dal provvedimento del Garante, sono impostati *alert* finalizzati a segnalare eventuali situazioni anomale emerse principalmente a seguito dell'analisi di:

1) fasce orarie di operatività (compresi orari, giorni non lavorativi e/o assenze);
2) accessi su rapporti non radicati o non gestiti presso/dalla struttura di appartenenza del dipendente;
3) ruolo dell'operatore;

L'alert è generato automaticamente quando tali parametri e/o una combinazione di essi superano una soglia prestabilita rispetto frequenze e livelli di riferimento definiti ad una normale operatività. Nel rispetto del principio della segregazione dei compiti previsti dalla normativa, i profili autorizzativi ed i diritti di accesso ai dati bancari sono adeguatamente gestiti e controllati, di conseguenza non possono verificarsi transazioni al di fuori dei ruoli organizzativi autorizzati.

L'accesso alle informazioni obbligatoriamente archiviate ed all'applicativo di generazione degli alert sarà consentito all'Ufficio Organizzazione ed Edp, nonché alle funzioni aziendali di controllo. Eventuali modifiche nella struttura organizzativa della Sardaleasing, potranno comportare modifiche alle denominazioni e/o al perimetro delle unità organizzative che accedono alle informazioni in parola: di tali modifiche si darà opportuna informativa.

In caso di generazione automatica di alert, le Strutture aziendali incaricate del presidio continuativo delle informazioni, qualora dovessero rilevare profili anomali, potranno segnalare alle funzioni aziendali di controllo ed alla Direzione Risorse Umane di Gruppo le situazioni di potenziale violazione della privacy e senza ritardo il dipendente verrà informato, senza che ciò costituisca avvio di procedura disciplinare ai sensi dell'art. 7 Legge 300, in merito alla verifica in corso e potrà essere sentito, anche su sua richiesta, con l'eventuale assistenza di un rappresentante sindacale dell'Organizzazione cui aderisce o conferisce mandato.

Gli accessi eseguiti da tali strutture sono a loro volta tracciati e conservati per i tempi di conservazione previsti all'art. 3 del presente accordo.