VERBALE DI ACCORDO SULL'APPLICAZIONE DEL PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI DEL 12 MAGGIO 2011, N. 192

In Roma, il giorno 19 aprile 2021 tra **BANCA UBAE S.p.A.,** rappresentata dai sigg.ri:

Maurizio Valfrè, Direttore Generale

e

la Delegazione Sindacale formata dalle seguenti Organizzazioni come sotto rappresentate:
– UGL Credito rappresentata dal sig. Giovanni Lippa

premesso che:

1) Banca UBAE S.p.A., (di seguito, **"Banca UBAE"**), in ottemperanza alle disposizioni emanate dal Garante per protezione dei dati personali c.d. Privacy (provvedimento n. 192 del 12 maggio 2011) relative alle nuove "*Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie*", ha avviato, anche di concerto con l'Outsourcer, la società Cedacri S.p.A., (di seguito, **"Cedacri"**), già nominata Responsabile del Trattamento dei Dati Personali, le attività di adeguamento dei sistemi e dei processi aziendali al fine di poter garantire il rispetto dei principi introdotti dal suddetto provvedimento, la cui entrata in vigore era prevista per il 30 settembre 2014 (provvedimento del Garante n. 257 del 22 maggio 2014);
2) Con particolare riferimento all'argomento di cui al punto che precede e al fine di favorire l'attuazione nei vari Istituti del citato Provvedimento del Garante per la protezione dei dati personali, ABI e Organizzazioni Sindacali Nazionali hanno sottoscritto l'Accordo Quadro 15.04.2014, 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;

3) 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. 13.08.2011 n. 138), i predetti accordi possono essere stipulati con gli organismi sindacali aziendali di cui all'art. 24 del CCNL 19.01.2012 o, se condiviso tra le parti, con la delegazione di gruppo di cui all'art. 25 dell'Accordo in materia di libertà sindacali del

07.07.2010, considerata la necessaria uniformità e il carattere eccezionale degli adempimenti connessi all'attuazione del Provvedimento del Garante";

4) 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, termine ultimo indicato dal Provvedimento del Garante n. 357 del 18 luglio 2013; in data 22 maggio 2014, lo stesso Garante ha emanato il Provvedimento n. 257 e ne ha differito il termine previsto per l'entrata in vigore al 30 settembre 2014".

5) In data 17 settembre 2014 nell'ambito dell'incontro annuale previsto dal CCNL di settore con le Delegazioni Sindacali, le stesse sono state informate circa il contenuto del Provvedimento del 12.05.2011 n. 192 del Garante per la Protezione dei dati personali e dell'accordo Quadro Nazionale del 15.04.2014 tra ABI e le Organizzazioni sindacali, ed i rappresentanti sindacali si sono espressi favorevolmente all'accordo sindacale ex art. 4, comma 2, L. n. 300 del 1970, per l'applicazione del Provvedimento.

6) In data 30 ottobre 2014 la Banca e le Rappresentanze aziendali hanno firmato un accordo per l'applicazione del provvedimento.

Ciò premesso, le Parti convengono quanto segue.

1) La premessa forma parte integrante e sostanziale del presente accordo;

2) Le Parti si danno atto del contenuto del Provvedimento e che lo stesso 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;

3) Il Provvedimento si applica a tutti i lavoratori incaricati dalla banca dei trattamenti riconducibili, nell'ambito di applicazione del Provvedimento n. 192, come chiarito nel successivo Provvedimento

n. 357 del 18 luglio 2013, quali che siano la qualifica, le competenze, gli ambiti di operatività e le finalità dei trattamenti che sono tenuti a svolgere;

4) Le Parti si danno atto, altresì, che il Provvedimento stabilisce che "*i file di log devono tracciare, per ogni operazione 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 (es. numero del conto corrente, fido/mutuo, deposito titoli)*";

5) Banca UBAE, in ottemperanza a quanto specificato al punto sub 4) che precede e in linea con le disposizioni di Vigilanza (Circolare 285/13, parte prima, Titolo IV, Capitolo 4, Sezione IV)[1], ha adottato, anche per il tramite della società Cedacri, adeguate soluzioni informatiche per la registrazione degli accessi, da parte degli utenti, alle funzionalità di tutte le applicazioni informatiche che consentono la visualizzazione e/o la modifica delle informazioni economico patrimoniali dei clienti.

Cedacri, tuttavia, prendendo spunto anche dalle linee guida di ABI Lab del dicembre 2013 e per dar modo agli Istituti di correlare con maggiore efficacia gli eventi originati dall'operatività quotidiana dei dipendenti bancari con lo scopo di ottenere degli alert significativi, minimizzando il potenziale impatto sulla successiva fase di analisi, oltre ai dati obbligatori riportati al punto sub 4), ha deciso di raccogliere numerose informazioni aggiuntive riguardanti le operazioni bancarie (così come definite nel testo del Provvedimento); a tal fine si allega il disegno dell'architettura e l'elenco completo dei dati raccolti (allegato 1 – fonte Cedacri).

---

[1] Le misure di sicurezza sono distribuite su diversi strati, così che un'eventuale falla in una linea di difesa sia coperta dalla successiva ("difesa in profondità"); esse comprendono: (omissis), il monitoraggio, anche attraverso l'analisi di log e tracce di audit, di accessi, operazioni e altri eventi al fine di prevenire e gestire gli incidenti di sicurezza informatica; le attività degli amministratori di sistema e altri utenti privilegiati delle componenti critiche sono sottoposte a stretto controllo; le regole di tracciabilità degli accessi e delle operazioni effettuate, finalizzate a individuare le attività anomale e a svolgere le relative indagini, nonché alla verifica a posteriori delle operazioni critiche, con l'archiviazione dell'autore, data e ora (5), contesto operativo e altre caratteristiche salienti della transazione. Le registrazioni sono conservate in archivi non modificabili o le cui modifiche sono puntualmente registrate per un periodo commisurato al livello di criticità delle funzioni aziendali, dei processi di supporto e delle risorse informatiche, documentato negli inventari aziendali (6).

(5) ai fini della possibilità di una corretta e agevole ricostruzione di eventi e operazioni che coinvolgono più sistemi, inclusi eventualmente sistemi esterni, è opportuno che l'intermediario si doti di un sistema unificato di riferimento temporale, ad es. basato sul protocollo standard NTP e sincronizzato con un segnale orario di riferimento ufficiale.

(6) Restano fermi gli obblighi di conservazione di dati e documenti previsti dalla normativa applicabile.

Nei chiarimenti del 18 luglio 2013 (Provvedimento n. 357), il Garante ha indirizzato il tema dell'accesso massivo ai dati della clientela, c.d. *"query massive"*, per le quali si intendono tutte le funzioni disponibili agli incaricati che, a seguito della digitazione in campi d'input di alcuni criteri di ricerca, possono fornire contestualmente in output risultati che contengono dati riferibili a più clienti, indicando alcune modalità di tracciamento ovvero:

- ✓ *i dati relativi all'incaricato che ha eseguito la query*
- ✓ *la data e l'ora*
- ✓ *il dettaglio della relativa richiesta*

oltre le succitate informazioni Cedacri ha deciso di tracciare ulteriori dati al fine di effettivo ausilio nell'identificazione di eventuali comportamenti anomali e nella loro analisi (allegato 1 – fonte Cedacri).

6) Sulle predette registrazioni è, inoltre, prevista l'attivazione di specifici sistemi di monitoraggio *(alert)* per l'individuazione di comportamenti potenzialmente anomali o a rischio relativi ad operazioni (anche di sola inquiry) effettuate dai dipendenti incaricati del trattamento, configurabili come intrusioni o accessi anomali ai dati bancari dei clienti, mediante l'utilizzo dei suddetti sistemi informatici aziendali e suscettibili di essere considerati trattamenti illeciti dei dati stessi;

7) Tutte le informazioni registrate vengono automaticamente catturate e mantenute in una specifica base dati dalla quale vengono automaticamente cancellate secondo una cadenza temporale 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.

8) Come specificatamente richiesto dal Garante, sono attivati in automatico dal sistema centralizzato di gestione *"specifici alert"* finalizzati ad individuare *"comportamenti anomali o a rischio"*, rilevati dal sistema stesso in funzione delle seguenti regole, ricavate sulla base di pronunciamenti in passato emessi dal Garante e dalle linee guida ABI Lab:

- ✓ *numero di accessi ai dati del singolo cliente, effettuati nella giornata dallo stesso incaricato, superiore a N;*
- ✓ *numero di accessi ai dati del singolo cliente, effettuati nella giornata da più incaricati, superiore a N;*
- ✓ *numero di accessi ai dati del singolo cliente, effettuati nell'unità di tempo dallo stesso incaricato, superiore a N;*
- ✓ *numero di accessi ai dati del singolo cliente, effettuati nell'unità di tempo da più incaricati, superiore a N;*

- ✓ *numero di accessi in circolarità, effettuati nella giornata dallo stesso incaricato, superiore a N;*
- ✓ *numero di accessi in circolarità, effettuati nell'unità di tempo dallo stesso incaricato, superiore a N.*

dove il valore N è inizialmente un numero deciso dalla società Cedacri (fonte Cedacri).

Tenuto conto della sperimentalità della materia, tale parametro cosi come la logica di costruzione degli alert e dei report potrà essere oggetto di modifiche e/o personalizzazione che potranno essere richieste alla società Cedacri; in occasione della prima verifica prevista al punto sub 13) dell'accordo, sarà fornita, sulla base dei rilievi nel frattempo effettuati, sia una casistica esemplificativa dei comportamenti definiti come *"anomali o a rischio"* sia un aggiornamento degli elementi tenuti in considerazione ai fini della definizione degli alert.

L'attività di controllo degli alert, ai sensi del Provvedimento del Garante, deve essere affidata "*a unità organizzativa e, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti*", in particolare viene identificata quale unità preposta a ricevere le segnalazioni del sistema di gestione centralizzato di cui sopra e ad effettuare, esclusivamente su tali segnalazioni, una valutazione sulle caratteristiche degli alert riscontrati, la funzione Direzione Organizzazione & IT (controlli di I livello), in ogni caso, si esclude che le informazioni in esame vengano utilizzate a fini gestionali delle risorse.

La stessa unità si interfaccerà con la società Cedacri e/o altre eventuali società per quanto riguarda gli aspetti organizzativi/tecnologici, di manutenzione e/o implementazione del sistema di tracciamento sulle nuove piattaforme applicative e del rispetto dei relativi requisiti e alla verifica della "*data quality*" per l'infrastruttura c.d. Garante II.

Il processo di "*data quality*' si applica a tutta l'infrastruttura del Garante II presente in Cedacri e si declina in componenti tecnologiche e processi organizzativi, i primi eseguono controlli di tipo formale sul dato (presenza, dimensione, tipo) nella fase di trattamento del dato precedente al caricamento sul repository del Garante, scartando record non conformi. I secondi hanno per lo scopo il controllo e le verifiche sulla correttezza, completezza e congruità del tracciamento dal punto di origine del dato fino alla sua consultazione. La "*data quality*" fa sì che i dati personali devono essere esatti, completi, aggiornati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5 Regolamento Europeo sulla protezione dei dati personali 2016/679 del 27.4.2016 (GDPR).

9) Qualora, nel corso delle analisi di cui sopra, ovvero a seguito di indagini rivenienti da istanze avanzate dalla clientela in forza dei diritti di cui agli artt. 15 e seguenti del Regolamento Europeo

sulla protezione dei dati personali 2016/679 del 27.4.2016 (GDPR), ovvero a seguito di richieste dall'Autorità Garante o di altra Authority legittimata, dovessero emergere profili di particolare gravità, la struttura Direzione Organizzazione & IT coinvolgerà nell'analisi della segnalazione e per le conseguenti rispettive verifiche, le seguenti ulteriori strutture, in successione:

- ✓ La Direzione Risorse Umane
- ✓ Il Responsabile interno del trattamento dei dati personali dei dipendenti (ove presente)
- ✓ La Direzione Generale della Banca
- ✓ La funzione di Audit

Nel caso di conferma dell'anomalia 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.

10) In relazione all'accesso massivo ai dati della clientela, c.d. *"query massive"* - denominazione con cui si intendono tutte le funzioni disponibili agli incaricati che, a seguito della digitazione in campi d'input di alcuni criteri di ricerca, possono fornire contestualmente in output risultati che contengono dati riferibili a più clienti - si segnala che la Banca, ad integrazione della soluzione tecnica per l'adempimento del provvedimento del garante di cui al punto 1), ha approntato uno strumento software denominato SADAS.

L'accesso alla sopra menzionata applicazione è riservato in via esclusiva al personale Audit ed al Responsabile della Sicurezza e Privacy, previo obbligatorio inserimento, nella videata iniziale del programma, delle relativi ragioni giustificatrici dell'accesso medesimo quali, in via esemplificativa e non esaustiva: l'osservanza delle disposizioni del Garante in materia di tracciamento delle *"query massive"*; l'adempimento di provvedimenti dell'Autorità; l'effettuazione di controlli difensivi diretti ad accertare, in presenza di motivato sospetto, comportamenti illeciti del dipendente; l'effettuazione di verifiche in presenza di anomalie segnalate da *alert* dell'applicazione; la risoluzione di problemi di sicurezza informatica generati da usi impropri/fraudolenti dei dati.

Ogni accesso all'applicativo SADAS è soggetto a registrazione di cui verrà tenuta memoria per il tempo strettamente necessario al conseguimento delle finalità a cui l'accesso medesimo sottende.

La Banca, ad espressa richiesta, renderà disponibile al dipendente autore delle *"query massive"* oggetto di consultazione mediante il software SADAS la lista degli accessi all'applicazione riferiti alla operatività dello stesso; la lista fornita al dipendente interessato riporterà anche le motivazioni

inserite dal personale Audit e/o dal Responsabile della Sicurezza e Privacy a giustificazione degli accessi effettuati.

I dati, che possono essere estratti dal database della Banca, oltre a quelli indicati nel provvedimento del garante e anche nella circolare Banca d'Italia 285/13 (capitolo IV sistemi informativi), consistono nella sola notazione tecnica della *query* eseguita e non forniscono, quindi, report di dettaglio ulteriori (ad esempio, circa i nominativi dei clienti interessati o in merito alle risultanze della *query*).

11) Banca UBAE, in coerenza a quanto espressamente stabilito dal Provvedimento, assicura che:

a) "*la gestione dei dati bancari deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte del titolare 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;*

b) *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* (articolo 4 comma 3 del provvedimento n. 192 del 12 maggio 2011), *sono svolte, altresì, verifiche periodiche sulla corretta conservazione dei file di log per il periodo previsto al punto 4.2.2"* (del provvedimento n. 192 del 12 maggio 2011).

c) *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.*

In linea con le indicazioni del Garante riportate al punto 4.1 e all'articolo 1 lettera e) del Provvedimento n. 192 del 12 maggio 2011, con le "Disposizioni di vigilanza per le banche in materia di conformità alle norme *(compliance)*" adottate dalla Banca d'Italia il 10 luglio 2007 e s.m.i. e con il sistema dei controlli interni (rif. Circolare 263 Banca d'Italia, 15° aggiornamento luglio 2013 par. 6) le attività relative ai punti succitati saranno assicurate dalla struttura di Audit (controlli di III livello), la struttura di Compliance della banca (controlli di II livello) si occuperà del controllo dei requisiti di conformità alle norme e collaborerà, come previsto dalle disposizioni succitate, con le altre funzioni aziendali (in particolare con la funzione di controllo interno, *c.d. internal auditing*)

12) La Banca, tramite le consuete modalità, provvederà a divulgare apposita informativa ai dipendenti per informarli delle nuove procedure e di ogni eventuale connesso adempimento.

13) A richiesta di una delle parti firmatarie si darà luogo ad incontri di verifica annuali in merito all'applicazione delle disposizioni di cui al presente accordo, tenuto conto della fase sperimentale in materia e degli aggiustamenti tecnico-organizzativi che potranno svilupparsi è previsto un primo

incontro di verifica, ulteriore rispetto all'incontro annuale succitato, entro il 31 dicembre 2020, ed avrà come oggetto la verifica congiunta della funzionalità del sistema anche alla luce dei primi dati disponibili sulla base degli alert pervenuti e dei controlli a campione effettuati. In tale occasione sarà valutata l'opportunità di procedere a specifiche attività di formazione da attivare nell'ambito di quanto previsto dall'art. 72 del vigente CCNL.

Nel caso in cui la Banca introduca significative variazioni agli strumenti di cui al presente accordo, si terranno incontri preventivi nel corso dei quali le Parti valuteranno congiuntamente la conseguente eventuale necessità di modificare e/o integrare il presente accordo.

14) Le parti si danno espressamente atto che 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.

15) Il sistema garantisce la riservatezza e l'inalterabilità delle informazioni secondo standard riconosciuti e l'accesso ai dati è riservato alle sole funzioni dedicate e preposte:

- ✓ Amministratori dello stesso sistema, per attività legate alla manutenzione/gestione (personale incaricato da CEDACRI)
- ✓ Utenti autorizzati facenti parte della Direzione Organizzazione & IT
- ✓ Compliance
- ✓ Audit

16) Per tutto quanto non espressamente previsto si rinvia all'Accordo Quadro Nazionale del 15 aprile 2014 ed ai Provvedimenti del Garante per la protezione dei dati personali richiamati e allegati alla presente.

Letto, confermato e sottoscritto

Banca UBAE S.p.A.

Il Direttore Generale _____

UGL CREDITO _____

Il presente accordo è costituito da n° 8 pagine e dell'allegato n°1 di n. 5 pagine.

Gli allegati sottoriportati, oltre il primo, costituiscono documentazione sulle fonti normative e accordi richiamati nel testo dell'accordo.

Lista Allegati:

Allegato 1: disegno dell'architettura e l'elenco completo dei dati raccolti

Allegato 2: Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie" (provvedimento n. 192 del 12 maggio 2011)

Allegato 3: Proroga del termine per l'adempimento delle prescrizioni di cui al Provvedimento n. 192 del 12 maggio 2011 in materia di circolazione delle informazioni bancarie - 22 maggio 2014 (provvedimento del Garante n. 257 del 22 maggio 2014)

Allegato 4: Chiarimenti in ordine alla delibera n. 192/2011 in tema di circolazione delle informazioni riferite a clienti all'interno dei gruppi bancari e 'tracciabilità' delle operazioni bancarie; proroga del termine per completare l'attuazione delle misure originariamente prescritte - 18 luglio 2013 (Provvedimento n. 357 del 18 luglio 2013)

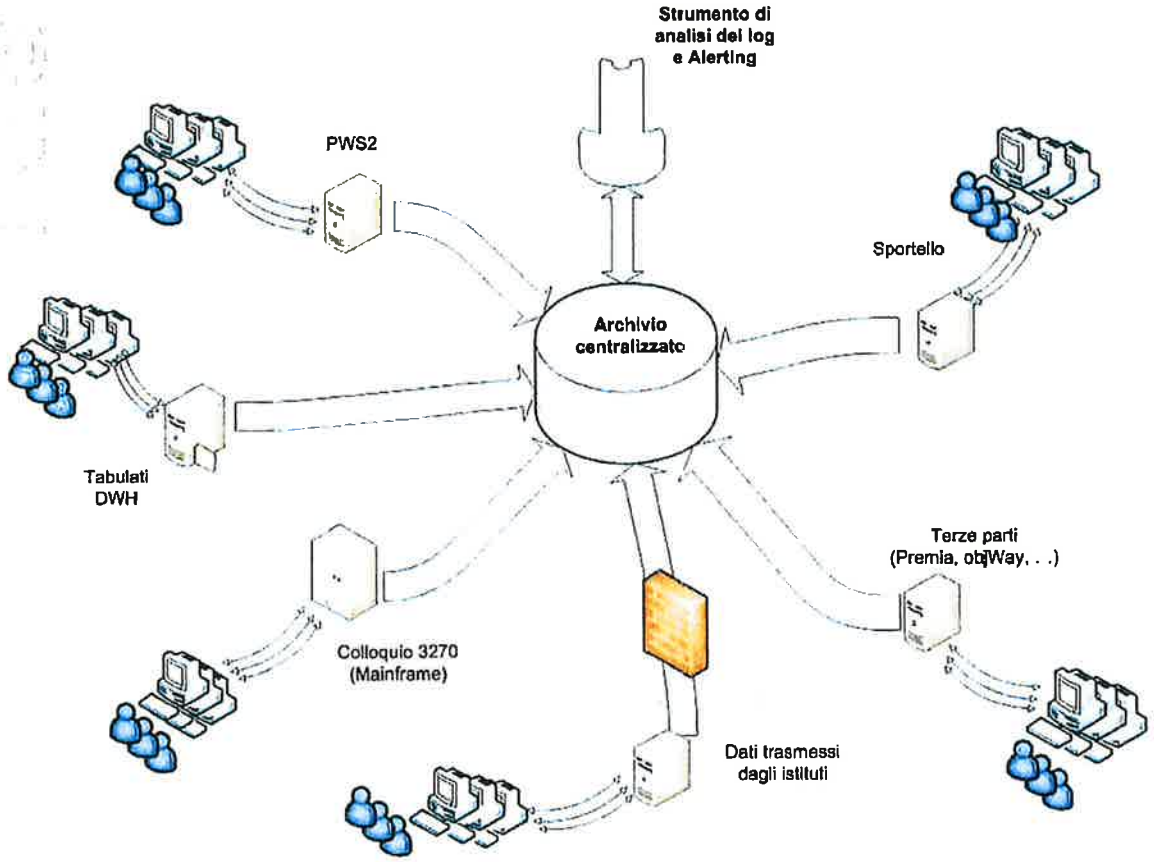
Allegato 5: Accordo Quadro nazionale su applicazione provvedimento del Garante n. 192 del 12 maggio 2011

ALLEGATO 1: disegno dell'architettura e l'elenco completo dei dati raccolti

1. DISEGNO ARCHITETTURALE

Nel sistema informativo Cedacri, il Provvedimento si traduce in uno strumento generalizzato per la raccolta dei "log" dei sottosistemi individuati come compresi all'interno del perimetro del provvedimento.

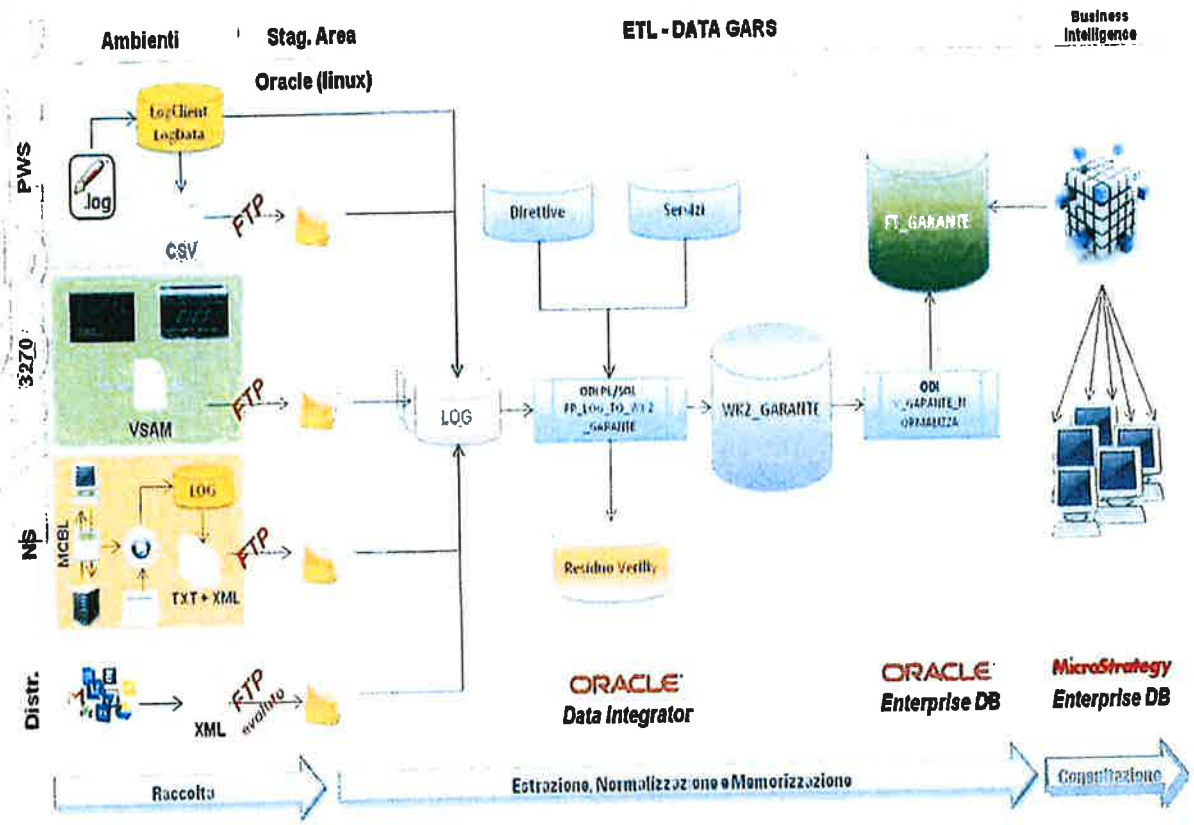
Le figure seguenti riassumono il disegno architetturale generale della soluzione Cedacri.



Si precisa altresì che Cedacri, nella progettazione e nell'implementazione della soluzione, ha seguito e segue le linee guida emesse dal Gruppo di Lavoro di ABILab (del quale Cedacri stessa fa parte).

Fonte Cedacri S.p.A.

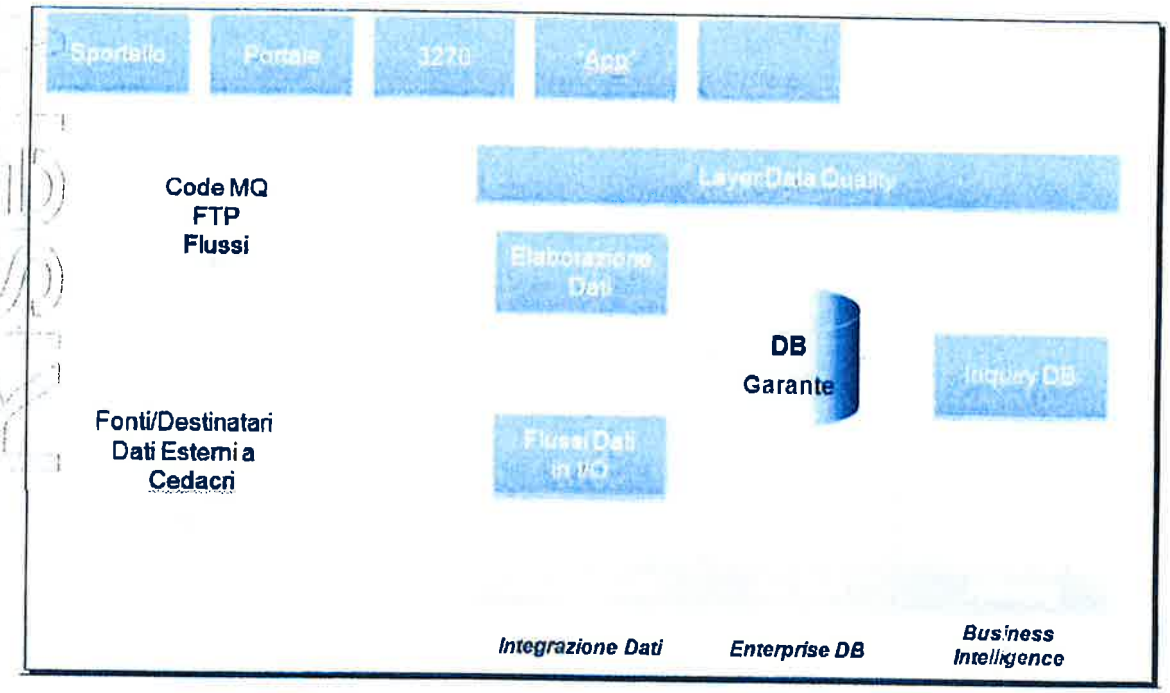
ALLEGATO 1: disegno dell'architettura e l'elenco completo dei dati raccolti



Fonte Cedacri S.p.A.

ALLEGATO 1: disegno dell'architettura e l'elenco completo dei dati raccolti

Dal punto di vista più strettamente applicativo la piattaforma è schematizzata come segue.



La soluzione custom prevista da Cedacri comporta la raccolta dei log effettuata nell'ambito dell'architettura applicativa con instradamento dei dati verso un "repository" centralizzato.

I sottosistemi applicativi che rientrano nel perimetro del provvedimento del Garante rappresentano una larga parte di quelli facenti parte del sistema informativo Cedacri.

Le informazioni minime da raccogliere, secondo le indicazioni del Provvedimento, sono:

- codice identificativo dell'incaricato;
- data e ora dell'operazione;
- postazione di lavoro utilizzata;
- codice cliente finale coinvolto;
- tipologia di rapporto contrattuale.

Cedacri, tuttavia, ha deciso di raccogliere numerose informazioni aggiuntive riguardanti le operazioni bancarie (così come definite nel testo del Provvedimento), per dar modo agli istituti di correlare con maggiore efficacia gli eventi originati dall'operatività quotidiana dei dipendenti bancari.
L'elenco completo dei dati raccolti viene presentato di seguito:

- La matricola dell'operatore che ha posto in essere la transazione
- Dominio di autenticazione della matricola in Active Directory
- La data e l'ora della richiesta
- Informazioni identificative del terminale: MAC Address
- Informazioni identificative del terminale: indirizzo IP (da HTTP Header)
- Informazioni identificative del terminale: IP (assegnato alla macchina)
- Informazioni identificative del terminale: TermID
- Computer name dell'origine
- NDG del cliente
- Codice del servizio
- Identificazione dell'Istituto

Fonte Cedacri S.p.A.

ALLEGATO 1: disegno dell'architettura e l'elenco completo dei dati raccolti

- Identificazione dell'istituto
- Codice CAB della filiale utilizzata dall'operatore
- Codice della filiale utilizzato o impostato dall'operatore
- Codice CAB della filiale presso la quale è acceso il rapporto del cliente oggetto dell'operazione
- Codice della filiale presso la quale è acceso il rapporto del cliente oggetto dell'operazione
- Codice del conto del rapporto in capo al cliente oggetto dell'operazione
- Indica se viene utilizzata una postazione HW oppure virtualizzata
- Identificativo della sessione di virtualizzazione
- Indica quale client è stato utilizzato (Browser, emulatore 3270, Mobile, ...)
- Sistema operativo del client utilizzato dall'operatore
- Caratteristiche del browser utilizzate dall'operatore
- Profilo TSS dell'operatore che esegue l'operazione
- Ruolo in Active Directory dell'operatore che esegue l'operazione
- Ruolo nella piattaforma utilizzata
- Ruolo definito dall'applicazione associato all'operatore che esegue l'operazione
- Identificativo della sessione operativa
- Codice identificativo dell'operazione posta in essere
- Codice funzione interno all'applicazione
- Specifica della funzione interna
- Importo dell'operazione dispositiva effettuata
- NDG dell'operatore che effettua l'operazione
- NDG del cliente per conto del quale viene effettuata l'operazione
- NDG del cliente che richiede l'operazione
- Piattaforma operativa
- Tipo addetto (profilo mainframe)
- Codice gestore cliente (da piattaforma consulenti)
- Responsabile (profilo mainframe)
- Esito dell'operazione

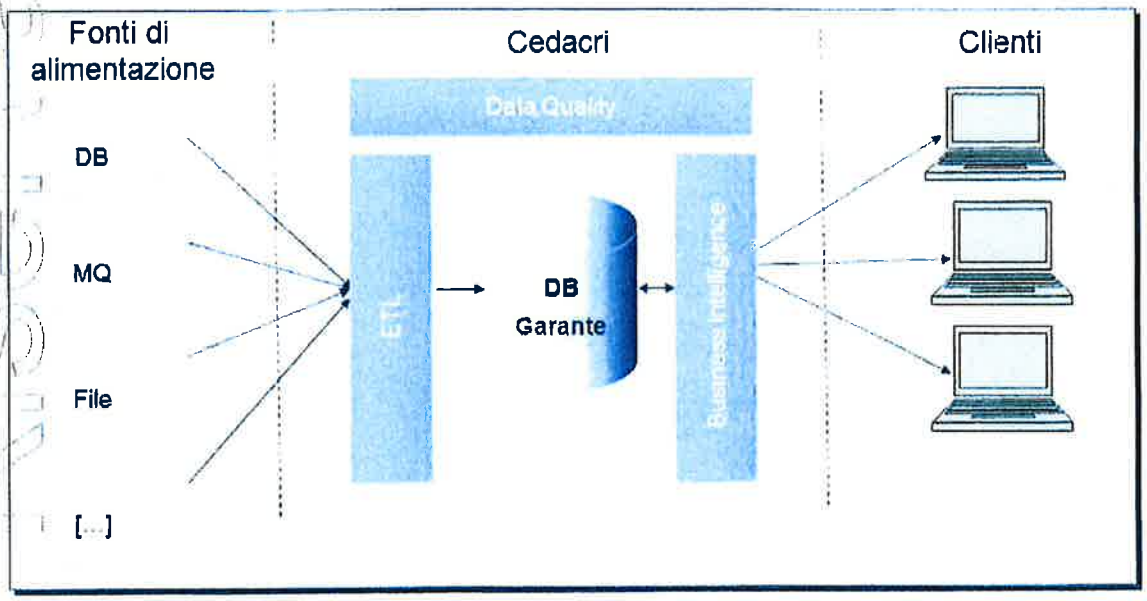
La presenza di molti dei dati raccolti dipende dalla piattaforma e dall'applicazione oggetto della tracciatura. Pertanto i dati aggiuntivi possono non essere sempre presenti nel log raccolto.

Come di seguito schematizzato, l'alimentazione da fonti esterne avverrà attraverso processi ETL[1] con il formato dei dati in input che dovrà rispettare il tracciato proposto da Cedacri. Attraverso il sistema di Business Intelligence sarà possibile eseguire interrogazioni e impostare alert sulla piattaforma dedicata al provvedimento.

1 ETL(Extract, Transform, Load) è un acronimo che identifica espressione il processo di estrazione, trasformazione e caricamento dei dati in un sistema di sintesi (data warehouse, data mart)

Fonte Cedacri S.p.A.

ALLEGATO 1: disegno dell'architettura e l'elenco completo dei dati raccolti



Nel caso di mappe o schermate che consentano un'interrogazione in grado di restituire risultati molteplici, si è deciso di tracciare, oltre al codice identificativo dell'operatore - data – ora, anche i seguenti dati:

RACCOLTA DATI RELATIVA ALLE "QUERY MASSIVE"

	Dati obbligatori	Dati facoltativi
Per le funzioni CICS	• Tipologia del rapporto (servizio) • ABI • Codice Istituto • Dati della query	• CAB operatore • Codice filiale operatore • Ruolo operatore applicativo • NDG operatore • Esito
Per le funzioni PWS2	• Funzione interna • Sottofunzione interna • Tipologia del Rapporto (Servizio) • ABI • Codice Istituto • Dati della query	• CAB operatore • Codice Filiale operatore • Ruolo operatore applicativo • NDG Operatore • Esito

La seguente documentazione è stata estratta dalla documentazione redatta e fornita dalla società dalla società Cedacri in particolar modo dal documento:
Presentazione Procedura – Garante II: tracciatura operatività

Fonte Cedacri S.p.A.