Gruppo Banca Privata Leasing

15 novembre 2023 – UniMC –Seminario Didattico

Il Ruolo della Compliance nel sistema dei controlli interni

Origine della Compliance

2005 - il Comitato di Basilea per la vigilanza bancaria introduce la norma sulla Compliance, la Funzione Compliance e la figura del Compliance Manager.

Perché? A seguito delle esperienze maturate dai clamorosi fallimenti in USA di multinazionali e società finanziarie, come il caso Enron, Lehman Brothers e altri.

Ci si rese conto che i modelli di governance sino ad allora adottati erano inadatti per garantire un controllo efficace della vita delle imprese e, conseguentemente, degli effetti sulla società.

Introduzione della Compliance nel sistema Bancario, Finanziario e Assicurativo

Nelle banche, negli intermediari finanziari e nel comparto assicurativo, la funzione di Compliance è chiamata a svolgere un ruolo complementare rispetto al sistema di gestione dei rischi previsto dalla regolamentazione prudenziale (Basilea, ecc…); la Compliance ha infatti un'ottica prevalentemente preventiva nel **presidiare rischi di carattere legale e reputazionale**.

Banche e intermediari che offrono servizi di investimento, bancari e assicurazioni devono obbligatoriamente istituire una funzione di compliance secondo le indicazioni fornite rispettivamente da:

- **Banca d'Italia** il 12 luglio 2007 nelle *"Disposizioni di Vigilanza – La funzione di conformità"*;
- **CONSOB** (congiuntamente a Banca d'Italia) il 29 ottobre 2007 nel *"Regolamento in materia di organizzazione e procedure degli intermediari che prestano servizi di investimento o di gestione collettiva del risparmio"*;
- **ISVAP** il 26 marzo 2008 nel *"Regolamento n.20 recante disposizioni in materia di controlli interni, gestione dei rischi, compliance (…)"*.

Tali normative di vigilanza recepiscono i principi guida sulla materia pubblicati nel **2005 dal Comitato di Basilea**. Molte aziende facenti parti di gruppi multinazionali specie se quotate in borsa, pur non essendo tenute a norma di legge, istituiscono una funzione di Compliance.

Il Sistema dei Controlli Interni

I controlli di terzo livello sono condotti dalla funzione di Internal Audit.

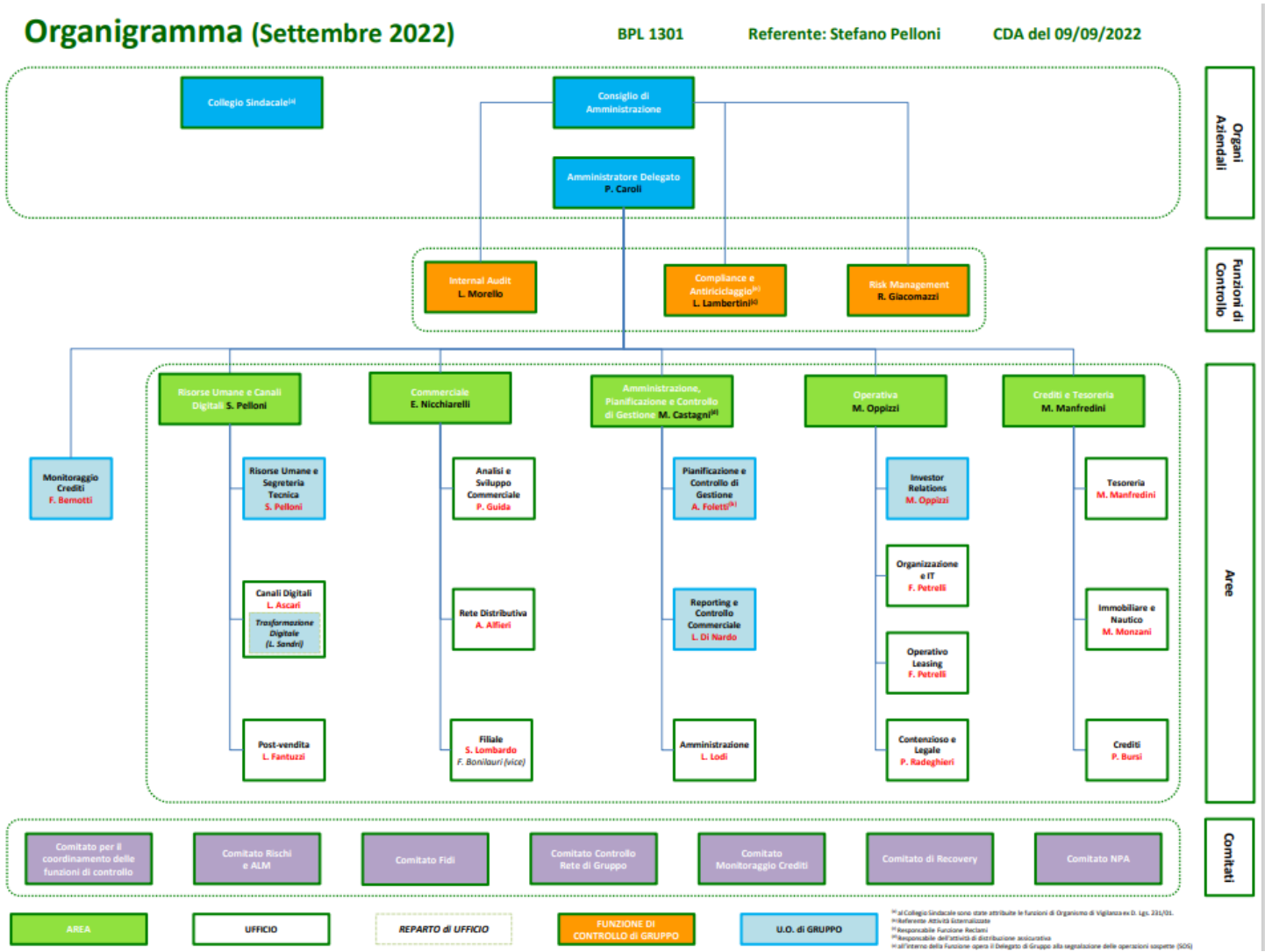
I controlli di secondo livello sono realizzati dalle funzioni di Risk Management, Compliance e AML

I controlli di linea e di processo sono garantite dalle singole funzioni operative e di business

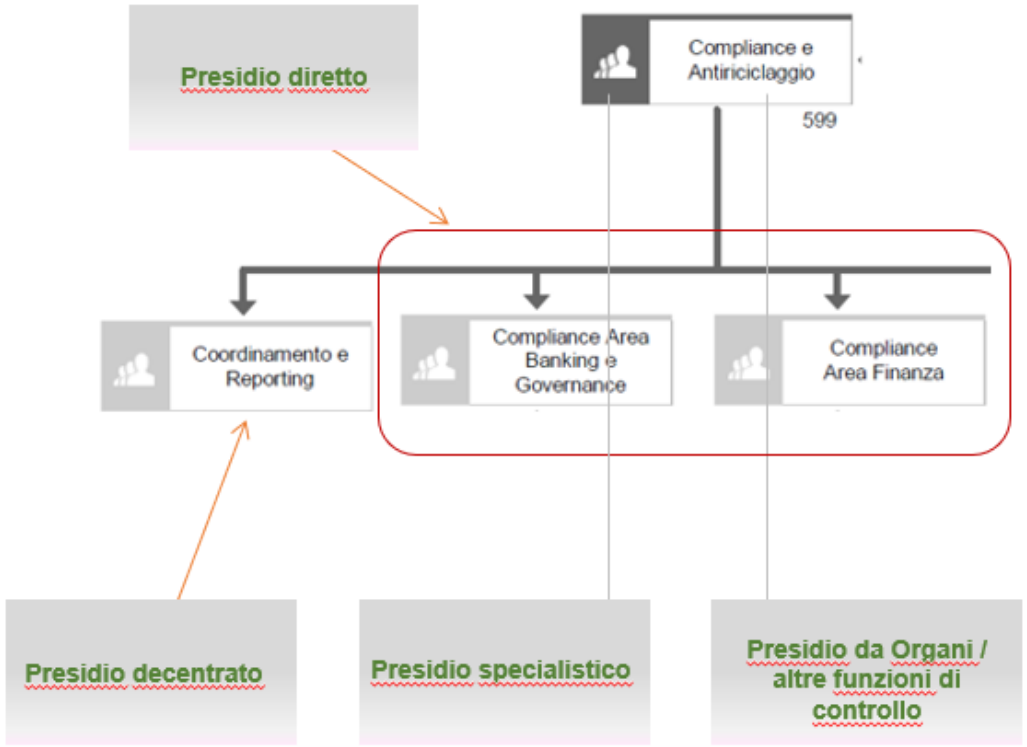
- Funzione Antiriciclaggio (AML/CTF)
- Funzione di controllo dei rischi ICT e di sicurezza (Agg. 40 Circ 285)

Organigramma

La Funzione di conformità alle norme (Compliance) è posta alle dirette dipendenze dell'organo con funzione di supervisione strategica, al quale riporta sia gerarchicamente che funzionalmente, preservando i raccordi con l'organo con funzione di gestione ed in particolare con l'Amministratore Delegato - Direttore Generale per quanto concerne aspetti amministrativi/gestionali ed informativi.



Modello organizzativo di Compliance



Le Disposizioni di Vigilanza per le Banche definiscono che la funzione di Compliance debba presiedere, secondo un approccio risk based, alla gestione del rischio di non conformità con riguardo a tutta l'attività aziendale.

Al fine di gestire il rischio di non conformità afferente l'intera attività svolta dalla Banca, il Responsabile della funzione di compliance si avvale:
- **presidio diretto:** da parte della Funzione per le norme più rilevanti e comunque poste a tutela del consumatore (relative all'ambito societario, ai servizi bancari ed ai servizi finanziari);
- **presidio decentrato:** da parte dei referenti di Compliance per le altre norme (es. Bilancio, segnalazioni di vigilanza) collocati presso le strutture operative della banca, i quali rispondono funzionalmente al Responsabile della funzione di Compliance con riferimento all'attività svolta per la funzione. Tali referenti agiscono sotto la guida dell'Unità Coordinamento e reporting che riporta gerarchicamente al Responsabile della funzione di Compliance;
- **presidio specialistico:** per gli ambiti normativi in materia di sicurezza sul lavoro, fiscale, nonché degli ambiti normativi inerenti altre società del Gruppo non soggette all'obbligo di istituzione della Funzione di Compliance;
- **presidio da organi/ altre funzioni di controllo:** ambiti normativi già presidiati dagli stesi (es. responsabilità degli enti ai sensi del D.Lgs. 231/01, Disciplina prudenziale di primo e secondo pilastro, Antiriciclaggio e antiterrorismo).

Il Rischio di «Non Conformità»

“Il rischio di non conformità alle norme è il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative (di legge o di regolamenti) ovvero di autoregolamentazione (es. statuti, codici di condotta, codici di autodisciplina).”

Funzione di conformità alle norme (compliance)

La Circolare n. 285 del 17 dicembre 2013 (Parte I – Recepimento in Italia della CRD IV; Titolo IV - Governo societario, controlli interni, gestione dei rischi; Capitolo 3 – Il sistema dei controlli interni; Sezione III – Funzioni aziendali di controllo) disciplina in particolare che:

«*Il rischio di non conformità alle norme è il rischio di incorrere (…). Poiché il rischio di non conformità alle norme è diffuso a tutti livelli dell'organizzazione aziendale, soprattutto nell'ambito delle linee operative,* ***l'attività di prevenzione deve svolgersi in primo luogo dove il rischio viene generato: è pertanto necessaria un'adeguata responsabilizzazione di tutto il personale****.*

La funzione di conformità alle norme presiede, ***secondo un approccio risk based****, alla gestione del rischio di non conformità con riguardo a tutta l'attività aziendale, verificando che le procedure interne siano adeguate a prevenire tale rischio.* ***A tal fine, è necessario che la funzione di conformità alle norme abbia accesso a tutte le attività della banca, centrali e periferiche, e a qualsiasi informazione a tal fine rilevante, anche attraverso il colloquio diretto con il personale****»*.

Funzione di conformità alle norme (compliance)

«I principali adempimenti che la funzione di conformità alle norme è chiamata a svolgere sono:

- *l'ausilio alle strutture aziendali per la definizione delle metodologie di valutazione dei rischi di non conformità alle norme;*
- *l'individuazione di idonee procedure per la prevenzione del rischio rilevato, con possibilità di richiederne l'adozione; la verifica della loro adeguatezza e corretta applicazione;*
- *l'identificazione nel continuo delle norme applicabili alla banca e la misurazione/valutazione del loro impatto su processi e procedure aziendali;*
- *la proposta di modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio dei rischi di non conformità identificati;*
- *la predisposizione di flussi informativi diretti agli organi aziendali e alle strutture coinvolte (ad es.: gestione del rischio operativo e revisione interna);*
- *la verifica dell'efficacia degli adeguamenti organizzativi (strutture, processi, procedure anche operative e commerciali) suggeriti per la prevenzione del rischio di non conformità alle norme».*

Funzione di conformità alle norme (compliance)

*«**Per le norme più rilevanti** ai fini del rischio di non conformità, quali quelle che riguardano l'esercizio dell'attività bancaria e di intermediazione, la gestione dei conflitti di interesse, la trasparenza nei confronti della clientela e, più in generale, la disciplina posta a tutela del consumatore, e per quelle norme per le quali non siano già previste forme di presidio specializzato all'interno della banca, **la funzione è direttamente responsabile della gestione del rischio di non conformità.***

*Con riferimento ad altre normative per le quali siano **già previste forme specifiche di presidio specializzato** (ad es.: normativa sulla sicurezza sul lavoro, in materia di trattamento dei dati personali), la banca, in base a una valutazione dell'adeguatezza dei controlli specialistici a gestire i profili di rischio di non conformità, può graduare i compiti della compliance, che comunque è responsabile, in collaborazione con le funzioni specialistiche incaricate, almeno della definizione delle metodologie di valutazione del rischio di non conformità e della individuazione delle relative procedure, e procede alla verifica dell'adeguatezza delle procedure medesime a prevenire il rischio di non conformità».*

Funzione di conformità alle norme (compliance)

«*La banca può adottare tale approccio anche con riferimento al presidio del rischio di non conformità alle* ***normative di natura fiscale****, che richiede almeno: (i) la definizione di procedure volte a prevenire violazioni o elusioni di tale normativa e ad attenuare i rischi connessi a situazioni che potrebbero integrare fattispecie di abuso del diritto, in modo da minimizzare le conseguenze sia sanzionatorie, sia reputazionali derivanti dalla non corretta applicazione della normativa fiscale; (ii) la verifica dell'adeguatezza di tali procedure e della loro idoneità a realizzare effettivamente l'obiettivo di prevenire il rischio di non conformità.*

Ferme restando le responsabilità della funzione di compliance per l'espletamento dei compiti previsti da normative specifiche *(quali, ad es., le discipline in materia di politiche e prassi di remunerazione e incentivazione, di trasparenza delle operazioni e correttezza delle relazioni tra intermediari e clienti e di attività di rischio e conflitti di interesse nei confronti di soggetti collegati),* ***altre aree di intervento sono****:* »

Funzione di conformità alle norme (compliance)

- *«il coinvolgimento nella **valutazione ex ante** della conformità alla regolamentazione applicabile di tutti i progetti innovativi (inclusa l'operatività in nuovi prodotti o servizi nell'ambito del relativo processo di approvazione, secondo quanto previsto nella Sezione II, paragrafo 3) che la banca intenda intraprendere nonché nella prevenzione e nella gestione dei conflitti di interesse sia tra le diverse attività svolte dalla banca, sia con riferimento ai dipendenti e agli esponenti aziendali;*

- *la **consulenza e assistenza nei confronti degli organi aziendali della banca** in tutte le materie in cui assume rilievo il rischio di non conformità nonché la collaborazione nell'attività di formazione del personale sulle disposizioni applicabili alle attività svolte, al fine di diffondere una cultura aziendale improntata ai principi di onestà, correttezza e rispetto dello spirito e della lettera delle norme.*

*Sotto il profilo organizzativo, tenuto conto dei molteplici profili professionali richiesti **per l'espletamento di tali adempimenti**, le varie fasi in cui si articola **l'attività della funzione di conformità alle norme possono essere affidate a risorse appartenenti ad altre strutture organizzative** (ad es., legale, organizzazione, gestione del rischio operativo), **purché il processo di gestione del rischio e l'operatività della funzione siano ricondotti ad unità mediante la nomina di un responsabile che coordini e sovrintenda alle diverse attività**».*

Valutazione del Rischio e rappresentazione agli Organi

La valutazione del rischio di non conformità avviene sulla base di criteri previsti all'interno di specifica Policy; ad esempio Policy "Modello di compliance e valutazione del rischio di non conformità".

In particolare, il rischio di non conformità (Rischio residuo) è determinato dalla combinazione di:

- ✓ Rischio inerente di non conformità, dato dalla combinazione del grado di esposizione al rischio e della probabilità di manifestazione del rischio stesso;

- ✓ Valutazione dei presidi adottati, data dalla combinazione delle verifiche di conformità normativa (ex ante) e dalle verifiche di conformità ex-post, basate sia sugli esiti dell'autovalutazione dei singoli responsabili sulle attività di propria competenza sia sulle verifiche effettuate direttamente dalla funzione di conformità, o indirettamente tramite l'Internal Audit in base all'accordo di servizio stipulato.

Valutazione del Rischio e rappresentazione agli Organi

ALBERO DEI PROCESSI GRUPPO BPL						
LIVELLO 1	LIVELLO 2	LIVELLO 3	LIVELLO 4	FASE	APPLICABILITA' SOCIETA' DEL GRUPPO BPL	OWNER
PROCESSI DI GOVERNO	PIANIFICAZIONE	ANALISI MACROECONOMICHE DI SETTORE	POSIZIONAMENTO COMPETITIVO DEL GRUPPO		SI, Banca Privata Leasing e ADV Finance	BPL: Ufficio Pianificazione e Controllo di gestione
PROCESSI DI GOVERNO	PIANIFICAZIONE	ANALISI MACROECONOMICHE DI SETTORE	BENCHMARK SISTEMA BANCARIO		SI, Banca Privata Leasing e ADV Finance	BPL: Ufficio Pianificazione e Controllo di gestione
PROCESSI DI GOVERNO	PIANIFICAZIONE	ANALISI MACROECONOMICHE DI SETTORE	ANALISI OBIETTIVI DI MERCATO		SI, Banca Privata Leasing e ADV Finance	BPL: Ufficio Pianificazione e Controllo di gestione
PROCESSI DI GOVERNO	PIANIFICAZIONE	PIANO STRATEGICO	ATTIVITÀ PREPARATORIA AL PIANO STRATEGICO		SI, Banca Privata Leasing e ADV Finance	BPL: Ufficio Pianificazione e Controllo di gestione
PROCESSI DI GOVERNO	PIANIFICAZIONE	PIANO STRATEGICO	ATTIVAZIONE DEL PIANO PIANO STRATEGICO		SI, Banca Privata Leasing e ADV Finance	BPL: Ufficio Pianificazione e Controllo di gestione

Ambito	Macroprocesso	Processo	Principale Area normativa di riferimento	Rischio inerente	Valutazione dei presidi				Rischio complessivo di non conformità	Interventi TdB aperti
					Rischio di non conformità ex -ante	Rischio di non conformità ex - post: Autovalutazione	Rischio di non conformità ex - post: Valutazioni di compliance	Rischio di non conformità lordo		
01 Governo e Gestione Rischi	01.01 Pianificazione Strategica	01.01.01 Definizione Strategie Aziendali	Sistema dei controlli interni	Medio - Alto	Parzialmente basso	Basso	-	Parzialmente basso	Parzialmente basso	
01 Governo e Gestione Rischi	01.01 Pianificazione Strategica	01.01.02 Corporate Social Responsability - Sostenibilità	Normative trasversali	Alto	Parzialmente basso	-	-	Parzialmente basso	In prevalenza alto	
01 Governo e Gestione Rischi	01.01 Pianificazione Strategica	01.01.03 Definizione e Gestione del Budget	Sistema dei controlli interni	Medio - Alto	Basso	Basso	-	Basso	Parzialmente basso	
01 Governo e Gestione Rischi	01.01 Pianificazione Strategica	01.01.04 Sviluppo nuovi prodotti, servizi, mercati, attività e gestione gamma prodotti (POG)	POG - Product Oversight Governance	Medio - Alto	Parzialmente basso	Parzialmente basso	-	Parzialmente basso	Parzialmente basso	
01 Governo e Gestione Rischi	01.01 Pianificazione Strategica	01.01.05 Partecipazioni	Partecipazioni detenibili dalle Banche	Medio - Basso	Basso	Basso	-	Parzialmente basso	Parzialmente basso	
01 Governo e Gestione Rischi	01.02 Governo dei rischi	01.02.01 RAF - Risk Appetite Framework	Sistema dei controlli interni	Alto	Basso	Basso	-	Basso	In prevalenza alto	
01 Governo e Gestione Rischi	01.02 Governo dei rischi	01.02.02 ICAAP	Disciplina Prudenziale: Primo Pilastro	Alto	Basso	Basso	Basso	Basso	In prevalenza alto	
01 Governo e Gestione Rischi	01.02 Governo dei rischi	01.02.03 ILAAP	disciplina Prudenziale: Requisiti di	Medio - Alto	Basso	Basso	Basso	Basso	Parzialmente	

Giudizio	Descrizione	Scoring
Medio	Il numero di requisiti nuovi o modificati nel periodo di riferimento dell'area normativa risulta compreso tra 10% e 30%	2
Basso	Il numero di requisiti nuovi o modificati nel periodo di riferimento dell'area normativa risulta inferiore o uguale al 10%	1

- Complessità normativa, commisurata al numero di requisiti normativi previsti per area normativa sulla base della seguente tabella.

Giudizio	Descrizione	Scoring
Alto	l'area normativa contiene > 400 requisiti	3
Medio	l'area normativa contiene tra i 100 e i 400 requisiti	2
Basso	l'area normativa contiene < 100 requisiti	1

Come riportato nel *framework* metodologico, il grado di esposizione al rischio e la probabilità di manifestazione sono valutati in base ad una scala a 3 livelli. Il loro incrocio determina il rischio inerente dell'area normativa analizzata su una scala a 4 livelli in base allo schema di seguito riportato:

		Probabilità di manifestazione del rischio			Rischio inerente
		Bassa	Media	Alta	
Grado di esposizione al rischio	Alto				Alto
	Medio				Medio - Alto
	Basso				Medio - Basso
					Basso

Attività della Compliance

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DELIBERA 6 ottobre 2022

Accreditamento dell'organismo di monitoraggio e approvazione del codice di condotta per i sistemi di informazione creditizia in tema di credito al consumo, affidabilita' e puntualita' nei pagamenti. (Provvedimento n. 324). (22A06239)

(GU n.258 del 4-11-2022)

IL GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI

Nella riunione odierna alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Fabio Mattei, segretario generale;

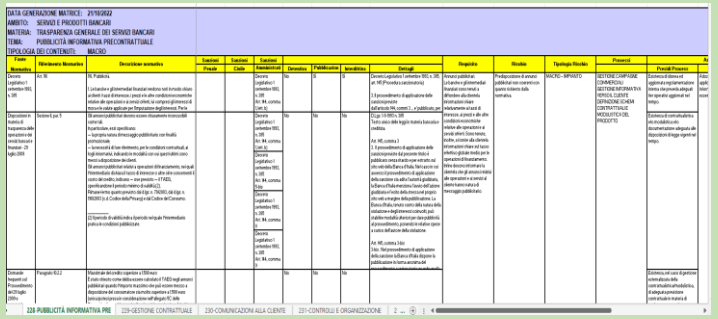
Visto il regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito, «regolamento»);

Visto il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito il «Codice») come novellato dal decreto legislativo 10 agosto 2018, n. 101 recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679»;

Visto l'art. 40 del regolamento che prevede che le associazioni e gli altri organismi rappresentanti le categorie di titolari o responsabili del trattamento possano elaborare (modificare o prorogare) codici di condotta destinati a contribuire alla corretta applicazione del regolamento in specifici settori di attivita' e in funzione delle particolari esigenze delle micro, piccole e medie imprese, e che tali codici devono essere approvati dall'autorita' di controllo competente;

Visto il considerando 98 del regolamento che prevede che tali codici possono calibrare gli obblighi del titolare e del responsabile del trattamento, tenuto conto dei potenziali rischi del trattamento per i diritti e le liberta' degli interessati;

Viste le «Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679»



Attività di Compliance

Attività di Compliance

Verifica Ex Ante – DDS, Rendiconti annuali CQ

Processo Supporto e Consulenza Legale e Tributaria
Responsabile documento Stefano Bodini (Responsabile Area Organizzazione e IT - ADV)

Premessa

Stefano Bodini – Responsabile Area Organizzazione e IT – richiede alla scrivente funzione quanto segue: *"(…) Come anticipato poco fa, il giro la bozza di layout che vorremmo usare per i rendiconti ADV e BPL per la CQ. Il file lo gestiremo noi quindi possiamo fare tutte le modifiche che riteniamo opportune e ben vengano eventuali osservazioni. Di nostro quello che possiamo dirti è che nella sezione avvisi comunicheremo al cliente l'eventuale cessione a Banche Cessionarie e forniremo le relative indicazioni sulla Banca e sulla gestione (se in carico a noi o alla banca).[1]".*

Verifica Ex Ante

Normativa di Riferimento

- Art.125-bis, comma 4 TUB – "Contratti e comunicazioni"[1];
- Art. 119, comma 1 TUB – "Comunicazioni periodiche alla clientela"[2];
- Par. 3.1 "Disposizioni di carattere generale"[3], Sez. IV "Comunicazioni alla clientela" Disposizioni di Trasparenza di Banca d'Italia;
- Par. 6.2 "Contenuto e modalità delle comunicazioni"[4], Sez. VII "Credito a Consumatori" Disposizioni di Trasparenza di Banca d'Italia.

Valutazioni
La scrivente funzione, analizzate le normative di riferimento, osserva che la bozza proposta necessita di alcuni aggiustamenti.

In particolare, premettendo che le disposizioni di trasparenza prevedo che annualmente al cliente vengano inviati due documenti:

- Il documento di sintesi (c.d. DDS) con la situazione relativa al finanziamento in essere al 31/12;

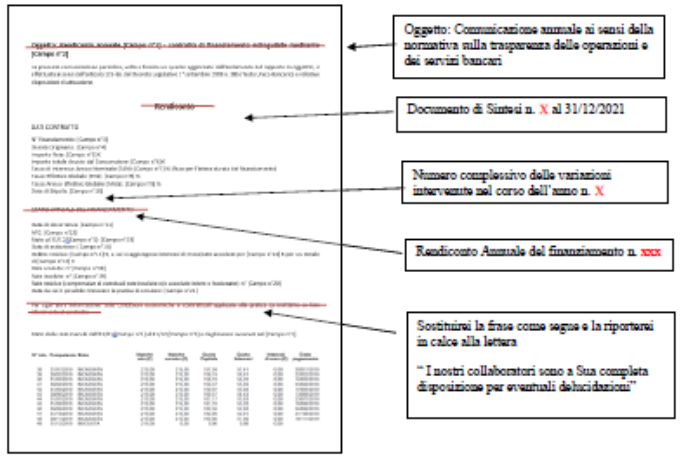
[1] Art. 125-bis, comma 4 TUB – "(…) 4. Nei contratti di credito di durata il finanziatore fornisce periodicamente al cliente, su supporto cartaceo o altro supporto durevole una comunicazione completa e chiara in merito allo svolgimento del rapporto. La Banca d'Italia, in conformità alle deliberazioni del CICR, fissa i contenuti e le modalità di tale comunicazione."
[2] Articolo 119, comma 1 TUB – "(…) 1. Nei contratti di durata i soggetti indicati nell'articolo 115 forniscono al cliente, in forma scritta o mediante altro supporto durevole preventivamente accettato dal cliente stesso, alla scadenza del contratto e comunque almeno una volta all'anno, una comunicazione chiara in merito allo svolgimento del rapporto. Il CICR indica il contenuto e le modalità della comunicazione".
[3] Par. 3.1 "Disposizioni di carattere generale"- "Nei contratti di durata gli intermediari forniscono ai clienti, alla scadenza del contratto e, comunque, almeno una volta all'anno, una comunicazione analitica che dia una completa e chiara informazione sullo svolgimento del rapporto e un quadro aggiornato delle condizioni economiche applicate (…).La comunicazione periodica è effettuata mediante invio o consegna di un rendiconto e del documento di sintesi delle condizioni economiche. (…). Il documento di sintesi, datato e progressivamente numerato, aggiorna quello unito al contratto (cfr. sezione II, paragrafo 7) e riporta le condizioni economiche in vigore. Le condizioni modificate rispetto alla comunicazione precedente sono riportate con una specifica evidenza grafica (ad esempio, attraverso l'uso del grassetto). Il documento di sintesi inviato con il rendiconto relativo al periodo che si conclude il 31 dicembre riporta inoltre il numero complessivo delle variazioni intervenute nel corso dell'anno".
[4] Par. 6.2 "Contenuto e modalità delle comunicazioni" – "Ai sensi dell'articolo 125-bis, comma 4, del T.U., nei contratti di credito di durata il finanziatore fornisce periodicamente al consumatore, su supporto cartaceo o su altro supporto durevole, una comunicazione completa e chiara in merito allo svolgimento del rapporto. La comunicazione è effettuata almeno una volta l'anno ed è volta ad assicurare che il consumatore abbia un quadro aggiornato dell'andamento del rapporto. Essa riporta ogni informazione rilevante a questo fine, nonché tutte le movimentazioni, anche mediante voci sintetiche di costo".

- Il Rendiconto del finanziamento al 31/12;

si evidenza come nel documento oggi proposto alla scrivente, lo stesso contenga le informazioni richieste dalla normativa ma lo stesso venga chiamato solamente "Rendiconto" e conseguentemente non differenzi le informazioni in esso contenuto rispetto a quanto previsto per o DDS e i Rendiconti. Altresì, il DDS fornito al cliente deve riportare:

- Il *"numero progressivo"* a partire da quello unito al contratto
- Il *"numero complessivo delle variazioni intervenute nel corso dell'anno"*.

Si propongono le seguenti modifiche:



Va ricordato che di norma il DDS e il Rendiconto annuale sono due comunicazioni separate.

La scrivente funzione, nel prendere atto che le presenti comunicazioni vengono per quest'anno (in relazione alle Cessioni del Quinto dell'anno 2021) effettuate in "casa" e dal prossimo anno automatizzate con l'ausilio dei sistemi dell'outsourcer CSE, ritiene possibile, visto la chiarezza delle stesse, inviarle in unico documento.

La scrivente funzione rimane in attesa di ricevere le eventuali comunicazioni aggiuntive previste nei casi di cessione al fine di valutarle.

Conclusione

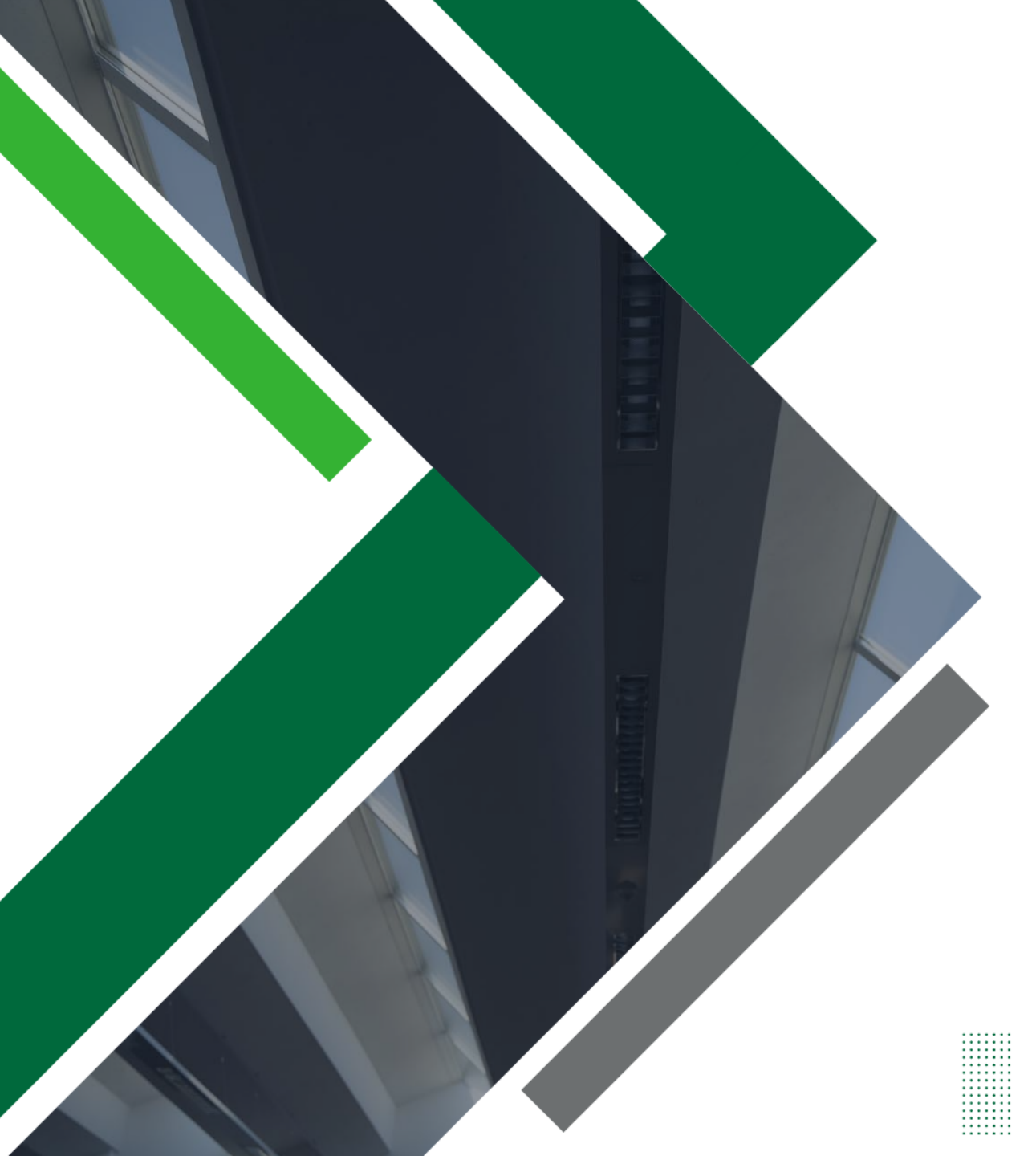
Giudizio delle attività esaminate: **Parzialmente Non Conforme**

Interventi richiesti - Raccomandazioni

Raccomandazione – far visionare alla scrivente il documento (DDS e Rendiconto relativi al 31/12/2021) per verificarne l'impostazione come sopra descritto e i testi delle eventuali comunicazioni aggiuntive previste nei casi di cessione.

Reggio Emilia, 04/11/2022

Il Responsabile Compliance e Antiriciclaggio di Gruppo
Luca Lamberti

Grazie
per l'attenzione

Luca Lambertini
Group Chief Compliance & AML Officer
Gruppo Banca Privata Leasing