DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Accordi di riservatezza (NDA): profili giuridici e implicazioni operative

19 Settembre 2025

Matteo Catenacci, Group General Counsel, Banca Investis

DB non solo diritto bancario

Matteo Catenacci, Group General Counsel, Banca Investis

Matteo Catenacci

Matteo Catenacci è Group General Counsel del Gruppo Banca Investis dal 2021, con responsabilità su legal & corporate affairs. In precedenza, ha collaborato con studi legali di primo piano, italiani e internazionali, affiancando intermediari finanziari, imprese assicurative e società fiduciarie su tematiche regolamentari e societarie.

1. Introduzione

In un contesto economico sempre più competitivo e interconnesso, la protezione delle informazioni riservate rappresenta una leva strategica per imprese, professionisti e operatori di mercato. Che si tratti di idee innovative, dati finanziari sensibili o relazioni commerciali in fase di sviluppo, la condivisione di contenuti privi di adeguate tutele può esporre l'organizzazione a rischi significativi, sia sotto il profilo economico che reputazionale.

Gli Accordi di Riservatezza – comunemente noti come NDA (Non-Disclosure Agreements) – costituiscono strumenti contrattuali essenziali per regolamentare la gestione delle informazioni confidenziali. La loro funzione è duplice: da un lato, delimitano l'ambito di utilizzo delle informazioni condivise; dall'altro, formalizzano l'impegno delle parti a non divulgarle a soggetti terzi.

La sottoscrizione di un NDA comporta obblighi giuridici ben definiti. In caso di violazione, la parte inadempiente può essere chiamata a rispondere civilmente per i danni causati e, in taluni casi, anche penalmente.

2. Ruolo dell'Accordo di Riservatezza (NDA)

Nel contesto delle relazioni professionali, commerciali e collaborative, l'NDA assume un ruolo centrale nella tutela delle informazioni confidenziali. Si tratta di uno strumento contrattuale che vincola una o più parti a non divulgare né utilizzare impropriamente i dati riservati acquisiti nel corso dell'interazione.

L'obiettivo principale dell'NDA è quello di:

(i) proteggere il know-how aziendale;

(ii) salvaguardare idee e progetti in fase di sviluppo;

(iii) tutelare dati sensibili e strategici;

(iv) prevenire danni economici, reputazionali o competitivi derivanti da divulgazioni non autorizzate.

Pur non essendo rigidamente disciplinato dalla legge, nella prassi contrattuale l'obbligo di riservatezza

vedi l'articolo online

si traduce in una serie di impegni che possono comportare sia comportamenti attivi (es. adozione di misure di sicurezza) sia doveri di astensione (es. non divulgazione).

In linea generale, è possibile distinguere due principali categorie di obblighi in capo alla parte ricevente: (1) obbligo di non divulgazione, che si concretizza nel divieto di comunicare le informazioni riservate a soggetti terzi e nella limitazione dell'accesso ai soli soggetti autorizzati, secondo il principio del *need to know*; (2) obbligo di protezione attiva, vale a dire adozione di misure tecniche e organizzative idonee a garantire la riservatezza e applicazione di standard di sicurezza proporzionati al valore e alla sensibilità delle informazioni.

2.1. *Obbligo di non divulgazione*

La parte ricevente si impegna a non comunicare né rendere accessibili a terzi le informazioni riservate ricevute nel corso del rapporto. Tale obbligo può articolarsi in diverse modalità, a seconda del livello di protezione richiesto:

(i) divieto assoluto di divulgazione: la parte ricevente non può in alcun modo condividere le informazioni, salvo consenso scritto e preventivo della parte divulgante;

(ii) divieto temperato: è consentita la trasmissione delle informazioni a soggetti specificamente individuati (es. dipendenti e consulenti), a condizione che siano essi stessi vincolati da obblighi di riservatezza equivalenti, che la divulgazione sia strettamente necessaria per l'esecuzione dell'attività e che venga applicato il principio del need to know, limitando l'accesso esclusivamente a chi ha effettiva necessità di conoscere i dati.

2.2. *Obbligo di protezione attiva*

La parte ricevente è altresì tenuta ad adottare misure tecniche e organizzative idonee a garantire la riservatezza delle informazioni ricevute. L'intensità dell'obbligo può variare in funzione del contesto operativo e del valore strategico dei dati:

(i) "ogni misura necessaria": implica l'adozione del massimo livello di protezione disponibile, anche superiore agli standard di settore, per prevenire qualsiasi rischio di accesso non autorizzato;

(ii) "misure ragionevoli sotto il profilo commerciale": richiede l'implementazione di strumenti proporzionati alla natura e alla sensibilità delle informazioni, tenendo conto delle best practice e delle risorse disponibili;

(iii) "misure equivalenti a quelle interne": impone alla parte ricevente di garantire un livello di protezione pari a quello applicato alle proprie informazioni riservate, assicurando coerenza e uniformità nella gestione dei dati.

Queste due categorie di obblighi costituiscono il cuore operativo di un NDA efficace. Una formulazione chiara, coerente e proporzionata è essenziale per garantire:

(i) tutela del patrimonio informativo aziendale;

(ii) conformità alle normative vigenti;

(iii) mitigazione di rischi legali e reputazionali.

3. Contenuti essenziali di un NDA

Per essere valido e giuridicamente vincolante, un NDA deve rispettare i requisiti generali previsti per ogni contratto.

Tuttavia, affinché sia realmente efficace, è fondamentale che contenga clausole specifiche e ben definite, capaci di delimitare con precisione l'ambito di applicazione e le responsabilità delle parti, evitando ambiguità interpretative.

Un NDA ben strutturato dovrebbe includere i seguenti elementi: identificazione delle parti; finalità dell'accordo; definizione di "informazioni riservate" ed esclusioni; ambito dell'obbligo di riservatezza; obblighi della parte ricevente; durata dell'accordo

3.1. *Identificazione delle parti*

Le parti contraenti devono essere chiaramente individuate, con eventuale estensione a terzi coinvolti (es. affiliati, agenti, consulenti).

vedi l'articolo online

Le parti sono generalmente definite come:

(i) "parte divulgante" (disclosing party), che condivide le informazioni riservate e deve assicurarsi che l'accordo sia sottoscritto prima della divulgazione;

(ii) "parte ricevente" (receiving party), che riceve le informazioni e si impegna a mantenerle riservate, utilizzarle solo per gli scopi previsti e restituirle o distruggerle su richiesta.

Gli NDA possono essere:

(i) unilaterali, quando solo una parte divulga informazioni riservate;

(ii) bilaterali, quando entrambe le parti di scambiano dati confidenziali.

La scelta dipende dalla natura del rapporto; un NDA unilaterale è preferibile in contesti più snelli e mirati.

3.2. *Finalità dell'accordo*

Una clausola che espliciti chiaramente lo scopo dell'NDA (es. le parti intendono condividere informazioni riservate esclusivamente per valutare una potenziale collaborazione commerciale) consente di circoscrivere il contesto applicativo e a prevenire interpretazioni estensive o improprie dell'accordo.

3.3. *Definizione di "informazioni riservate" ed esclusioni*

È opportuno includere nella definizione di "informazioni riservate" i dati scritti, orali o digitali, anche se non contrassegnati come confidenziali (es. piani di marketing, modelli operativi, dati finanziari). Nel contesto di progetti innovativi, possono essere considerate riservate, e quindi tutelabili, le informazioni tecniche, strategiche e operative contenute nella documentazione interna (es. manuali operativi, specifiche funzionali di servizi o prodotti, procedure interne, modelli di business non pubblici).

La definizione deve essere ragionevole e giustificabile, evitando formulazioni eccessivamente generiche che potrebbero risultare inapplicabili o contestabili.

Queste informazioni possono essere qualificate come know-how o segreti commerciali, se soddisfano i seguenti requisiti: (i) non devono essere di dominio pubblico (cd. segretezza effettiva); (ii) possiedono un valore economico (in termini di vantaggio competitivo) derivante dalla riservatezza; (iii) sono protetti da misure adeguate e ragionevoli, sia fisiche che giuridiche, per garantirne la riservatezza[1].

La previsione di esclusioni vale a dire informazioni riservate non soggette però a obbligo di riservatezza, tutela la parte ricevente da responsabilità ingiustificate e garantisce l'equilibrio contrattuale. Esempi di esclusioni sono: (i) informazioni già note alla parte ricevente[2]; (ii) informazioni di dominio pubblico[3]; (iii) informazioni sviluppate autonomamente[4]; (iv) informazioni ricevute da terzi senza obbligo di riservatezza; (v) informazioni richieste da autorità giudiziaria[5].

3.4. *Ambito dell'obbligo di riservatezza*

L'ambito dell'obbligo di riservatezza comprende le modalità di protezione delle informazioni (es. crittografia, accessi limitati), i contesti di utilizzo consentiti nonché i soggetti autorizzati all'accesso. Clausole troppo ampie o che limitano eccessivamente l'uso delle informazioni possono risultare invalide in alcune giurisdizioni.

1 Controllo degli accessi basato sui ruoli (RBAC); log di accesso che consentano la tracciabilità di creazione, visualizzazione, modifica e riproduzione; watermark automatici dei documenti come "riservati" o "confidenziali" e protezione con password condivise su canali separati; firewall e VPN a protezione della rete aziendale e dei documenti tramite protocolli criptati; blocco delle porte USB non autorizzate e disattivazione di archiviazione remota; inibizione di siti di trasferimento file e OCR pubblici; limitazione della condivisione interna ed esterna dei documenti riservati; sensibilizzazione per i dipendenti coinvolti in un progetto; clausole di riservatezza nei contratti.

2 Se la Parte Ricevente ha già ricevuto le stesse informazioni da una fonte indipendente prima della sua divulgazione, non può essere obbligata a mantenerle riservate.

3 Le informazioni già conosciute dalla Parte Ricevente o rese pubbliche (senza violazione dell'accordo) non possono essere considerate riservate (es. se un dipendente pubblica accidentalmente un documento riservato, è difficile far valere l'NDA su altri che lo ricevano successivamente).

4 Se la Parte Ricevente ha sviluppato autonomamente le stesse informazioni prima della sua divulgazione, non possono essere considerate confidenziali ai sensi dell'NDA.

5 Se un tribunale o un'autorità impone la divulgazione, la Parte Ricevente può essere obbligata a violare l'NDA. È buona prassi prevedere che la Parte Ricevente avvisi tempestivamente l'altra parte per consentirle di richiedere misure protettive.

vedi l'articolo online

3.5. *Obblighi della parte ricevente*

È buona prassi prevedere con chiarezza gli obblighi della parte ricevente (mantenere la riservatezza e non utilizzare impropriamente le informazioni), soprattutto al termine della relazione con la parte divulgante (restituire o distruggere i dati su richiesta e, comunque, non conservarne copia o archivi non autorizzati).

3.6. *Durata dell'accordo*

La durata dell'accordo, generalmente compresa tra 2 e 5 anni, può essere variabile in base al settore e alla sensibilità dei dati. La durata deve essere proporzionata al valore strategico delle informazioni trattate[6].

In aggiunta alla durata degli obblighi di riservatezza, viene solitamente prevista anche una clausola di sopravvivenza degli obblighi stessi, che continueranno ad avere efficacia anche dopo la cessazione del rapporto contrattuale tra le parti, per un periodo di tempo dalla data di cessazione, o fino a quando le informazioni riservate non diventino di pubblico dominio per cause non imputabili alla parte ricevente.

Resta inteso che l'obbligo di non divulgazione e di non utilizzo improprio delle informazioni riservate sopravvive alla scadenza o risoluzione dell'accordo, indipendentemente dalla causa della cessazione.

3.7. *Clausole aggiuntive (facoltative)*

A seconda del contesto e della natura delle informazioni condivise, l'NDA può essere integrato con ulteriori disposizioni volte a rafforzare la tutela delle parti e a prevenire comportamenti opportunistici.

Tra le più rilevanti:

(i) clausola di non sollecitazione del personale: questa clausola mira a impedire che una parte recluti o tenti di reclutare dipendenti, collaboratori o consulenti dell'altra parte. È opportuno limitarne l'applicazione ai casi in cui la sollecitazione derivi direttamente dalla conoscenza di informazioni riservate acquisite durante la collaborazione. La durata dell'obbligo può variare, ma generalmente si estende per 12-24 mesi dopo la cessazione del rapporto;

(ii) clausola di non circumvention (non elusione): particolarmente utile in ambiti commerciali, finanziari o di intermediazione, questa clausola - spesso accompagnata alla clausola di non sollecitazione del personale – impedisce che una parte aggiri l'altra per trarre vantaggio diretto da contatti, opportunità o relazioni acquisite nel corso della collaborazione. È consigliabile definire chiaramente i "contatti protetti" (es. clienti, investitori, partner strategici), stabilire una durata dell'obbligo (solitamente da 12 a 36 mesi), prevedere penali o risarcimenti in caso di violazione;

(iii) legge e giurisdizione applicabile: clausola fondamentale per evitare incertezze interpretative e contenziosi, anche transfrontalieri. È buona prassi specificare chiaramente la legge che regolerà l'accordo, indicare il tribunale competente o prevedere una clausola arbitrale o di mediazione internazionale, evitare formulazioni ambigue come "le parti si riservano di individuare la giurisdizione competente", preferendo i riferimenti espliciti alla normativa anche internazionale applicabile.

4. Presidi a garanzia della riservatezza

Una volta sottoscritto l'NDA da parte di un soggetto legittimato a impegnare l'azienda, la parte ricevente assume la responsabilità di gestire in modo corretto e sicuro le informazioni confidenziali ricevute. Per garantire un'efficace tutela della riservatezza, è necessario adottare un insieme coordinato di misure organizzative, tecniche e comportamentali. La parte divulgante dovrebbe essere in condizione di verificare in ogni momento la corretta gestione delle informazioni divulgate.

Di seguito un elenco pratico delle possibili misure operative da adottare in ambito aziendale:

(i) estensione degli obblighi di riservatezza con dipendenti, consulenti, fornitori e partner commerciali, inserendo clausole specifiche per la gestione di dati sensibili, know-how e documenti strategici;

6 Ad esempio, è buona norma distinguere tra informazioni confidenziali (protette per 2 anni) e segreti commerciali (protetti a tempo indefinito).

vedi l'articolo online

(ii) classificazione delle informazioni, etichettando i documenti come "confidenziali", "interni" o "pubblici" e utilizzando watermark, codici o sistemi di marcatura per identificare i contenuti riservati;

(iii) controllo degli accessi, implementando sistemi basati su ruoli e sul principio del need to know, monitorando e registrando gli accessi a sistemi informatici e archivi documentali;

(iv) formazione e sensibilizzazione del personale, organizzando corsi periodici su sicurezza informatica, protezione dei dati e compliance, promuovendo la cultura della riservatezza e la consapevolezza dei rischi legati alla divulgazione non autorizzata;

(v) controllo delle comunicazioni esterne, regolamentando l'uso di e-mail, social media e piattaforme di messaggistica e prevedendo approvazioni interne per la diffusione di contenuti sensibili;

(vi) gestione sicura dei dispositivi aziendali e dei dati digitali, proteggendo laptop, smartphone e supporti fisici con crittografia e password, vietando l'uso di dispositivi personali per attività aziendali senza autorizzazione, utilizzando firewall, antivirus, VPN e sistemi di backup sicuri, applicando policy di Data Loss Prevention (DLP) e crittografia end-to-end[7];

(vii) gestione e archiviazione dei documenti cartacei in luoghi sicuri, distruzione di quelli obsoleti con metodi certificati e limitazione della stampa di materiali riservati;

(viii) clausole di riservatezza nei contratti di uscita con ex dipendenti e collaboratori, e monitorando eventuali rischi di fuga di informazioni dopo la cessazione del rapporto;

(ix) gestione degli accessi fisici, registrando e accompagnando i visitatori in aree sensibili, limitando l'accesso a uffici, sale server e archivi al solo personale autorizzato[8].

7 Nel contesto attuale, l'intersezione tra obblighi di riservatezza e cybersecurity è diventata un pilastro imprescindibile per la protezione delle informazioni sensibili. Un NDA, da solo, non è sufficiente: deve essere integrato da misure tecniche e organizzative che ne garantiscano l'effettiva applicazione.

8 L'integrazione tra obblighi di riservatezza e il concetto di Chinese Walls è cruciale nei contesti ad alta sensibilità informativa, come banche d'investimento, studi legali, società di consulenza e gruppi industriali multi-business.

5. Coinvolgimento di terze parti

Nel contesto della gestione delle informazioni riservate, è fondamentale considerare il ruolo delle terze parti che, pur non essendo firmatarie dirette dell'NDA principale, possono accedere a dati sensibili. Collaboratori esterni, partner commerciali, investitori, fornitori, sviluppatori o consulenti tecnici rappresentano potenziali punti di vulnerabilità se non adeguatamente vincolati da obblighi di riservatezza.

Quando soggetti esterni accedono a informazioni strategiche, devono essere vincolati a:

(i) non divulgare le informazioni a soggetti non autorizzati;

(ii) non utilizzare i dati per finalità diverse da quelle previste dal contratto o dall'incarico;

(iii) adottare misure tecniche e organizzative adeguate per prevenire accessi non autorizzati.

Questi obblighi possono derivare da:

(i) clausole contrattuali specifiche nei contratti con terze parti, redigendo NDA separati, soprattutto in caso di scambio di informazioni strategiche;

(ii) normative settoriali, ad esempio il GDPR per la protezione dei dati personali;

(iii) principi generali di correttezza e buona fede nei rapporti commerciali.

I principali punti critici da monitorare riguardano il possibile accesso non controllato da parte di un terzo soggetto, che coinvolga subfornitori e collaboratori non vincolati da NDA, la condivisione informale mediante l'uso di canali non sicuri (es. e-mail personale, cloud non aziendale) e la mancanza di chiarezza se l'obbligo di riservatezza persiste anche dopo la cessazione del rapporto contrattuale.

A livello di best practice, è opportuno effettuare una due diligence preventiva sulla terza parte prima della condivisione di informazioni, prevedere audit e verifiche periodiche sul rispetto degli obblighi

Mentre l'NDA impone obblighi giuridici di riservatezza, le Chinese Walls rappresentano barriere interne che ne garantiscono l'effettiva applicazione.

vedi l'articolo online

contrattuali e integrare la riservatezza nei codici etici e nelle policy aziendali, rendendola parte integrante della cultura organizzativa.

6. Obblighi di riservatezza e Modello 231/2001

Da ultimo, è utile una breve riflessione sulla connessione tra obblighi di riservatezza e tutela dell'integrità aziendale nel contesto della disciplina della responsabilità ex D.Lgs. 231/2001.

L'NDA rappresenta una leva fondamentale per la prevenzione dei reati. L'NDA, infatti, non è solo uno strumento contrattuale, ma può diventare parte integrante del sistema di compliance.

In particolare, l'NDA può essere uno strumento operativo del Modello 231/2001, contribuendo a:

(i) prevenire la divulgazione illecita di informazioni riservate (es. segreti industriali, dati personali, piani strategici);

(ii) limitare il rischio di concorrenza sleale, appropriazione indebita o abuso di informazioni privilegiate;

(iii) rafforzare la protezione contro reati informatici e violazioni del GDPR, integrando misure di sicurezza e controllo.

L'inserimento dell'NDA tra i protocolli del Modello 231/2001 consente la formalizzazione di obblighi di riservatezza nei contratti con dipendenti, consulenti e terze parti, la tracciabilità delle dichiarazioni e delle verifiche e il coinvolgimento dell'Organismo di Vigilanza (OdV) nella gestione delle segnalazioni e dei controlli.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it