

**MODELLO DI
ORGANIZZAZIONE,
GESTIONE E CONTROLLO**

ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

PARTE SPECIALE N

**DELITTI IN MATERIA DI
DIRITTO D'AUTORE**

INDICE

1.	FUNZIONE DELLA PARTE SPECIALE N.....	3
2.	LE FATTISPECIE DEI DELITTI IN MATERIA DI DIRITTO D'AUTORE.....	4
2.1.	Le singole tipologie di reato.....	4
3.	ATTIVITÀ SENSIBILI NELL'AMBITO DEI DELITTI IN MATERIA DI DIRITTO D'AUTORE.....	5
3.1.	Le Attività sensibili.....	5
3.2.	Organi e funzioni aziendali coinvolti.....	5
4.	PRINCIPI E REGOLE GENERALI DI COMPORTAMENTO	7
4.1	Regole generali di comportamento.....	7
4.2	Regole specifiche di comportamento	9
4.3.	Policy e procedure specifiche.....	10
5.	I CONTROLLI DELL'ORGANISMO DI VIGILANZA.....	11

1. FUNZIONE DELLA PARTE SPECIALE N

La presente Parte Speciale si riferisce a comportamenti posti in essere dai dipendenti e dagli Organi Sociali di FriulAdria, nonché dai suoi collaboratori esterni e dai suoi *Partner* come già definiti nella Parte Generale.

Obiettivo della presente Parte Speciale è che tutti i Destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi degli illeciti in essa considerati.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- indicare i principi procedurali e le regole di comportamento che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza, e ai responsabili delle altre funzioni aziendali che cooperano con tale organismo, gli strumenti esecutivi necessari affinché gli stessi possano esercitare le attività di controllo, monitoraggio e verifica.

La Banca adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione dei reati di seguito descritti.

2. LE FATTISPECIE DEI DELITTI IN MATERIA DI DIRITTO D'AUTORE

2.1. Le singole tipologie di reato

L'art. 15, comma 7 lettera c) della legge 23 luglio 2009, n. 99 ha esteso la responsabilità amministrativa degli enti ai seguenti delitti in materia di violazione del diritto d'autore:

- **Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa** (art. 171, l. 633/1941 comma 1 lett a) bis);
- **Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione** (art. 171, l. 633/1941 comma 3);
- **Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori** (art. 171-bis l. 633/1941 comma 1);
- **Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati** (art. 171-bis l. 633/1941 comma 2);
- **Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa** (art. 171-ter l. 633/1941);
- **Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione** (art. 171-septies l. 633/1941);
- **Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale** (art. 171-octies l. 633/1941).

3. ATTIVITÀ SENSIBILI NELL'AMBITO DEI DELITTI IN MATERIA DI DIRITTO D'AUTORE

3.1. Le Attività Sensibili

Nell'ambito delle attività sociali che possono comportare la commissione di uno dei delitti in materia di diritto d'autore di cui all'art. 25 - *nonies* del D.lgs. 231/01 sono state individuate le Attività Sensibili che si vanno ad indicare.

La Società – richiamato quanto già esposto alla Parte Speciale I sui delitti informatici - ritiene opportuno regolamentare l'utilizzo delle proprie risorse informatiche per assicurare che in tale ambito non vengano poste in essere condotte in violazione delle norme sul diritto d'autore.

In particolare, a seguito della migrazione dal Gruppo Intesa al Gruppo Crédit Agricole, può risultare difficoltoso verificare l'attuale validità delle licenze software in essere, in quanto originariamente acquistate dal gruppo cedente *"in pacchetti"*.

Un ulteriore rischio con riferimento ai reati presupposto in esame deriva dal fatto che la Banca utilizza un canale televisivo web. Sebbene abbiano accesso allo stesso solamente i dipendenti (e non un pubblico indifferenziato) e la trasmissione sia riservata esclusivamente a contenuti istituzionali ed informativi, vi è l'esigenza che siano adottate adeguate procedure che assicurino che sulla Web TV non siano trasmessi contenuti che si pongano in violazione della normativa di cui alla presente Parte Speciale.

Talvolta, accade poi che la Banca a scopo promozionale organizzi convention od eventi a cui partecipano artisti musicali, o che utilizzi per proprie pubblicazioni (ad esempio, pubblicità, agende, libri strena ecc.) fotografie o quadri. Anche in questi casi, è ravvisata la necessità di adottare procedure che assicurino la legittimità di tali attività sotto il profilo del diritto d'autore.

3.2. Organi e funzioni aziendali coinvolti

Per quanto riguarda le Aree Sensibili riferibili all'utilizzo delle risorse informatiche, si ritengono particolarmente coinvolti alcuni organi e funzioni aziendali o della Capogruppo.

Per le attività svolte in service, regolate da specifico Contratto di Servizio (Service Agreement), è previsto un referente presso le rispettive strutture, autorizzato ad intrattenere i rapporti relativi alla fornitura del servizio.

A) Funzioni di Cariparma che operano anche per FriulAdria:

(i) Direzione Sistemi Informativi

(ii) Ufficio Acquisti

L'Ufficio Acquisti effettua gli ordini relativi all'acquisto ed alla sottoscrizione di nuove licenze.

(iii) Servizio Sicurezza

È la funzione che presidia e gestisce la sicurezza informatica per tutto il Gruppo.

(iv) Ufficio Comunicazione Interna

È la funzione che gestisce la comunicazione interna del Gruppo, in accordo con la funzione Risorse Umane, anche attraverso specifici strumenti, fra i quali la Web TV di Gruppo.

(v) Ufficio Eventi e Sponsorizzazioni

È l'ufficio cui spetta l'organizzazione degli eventi e delle iniziative del Gruppo rivolte al pubblico, gestendone gli aspetti logistici e organizzativi.

B) Funzioni di FriulAdria

(i) Servizio Personale e Organizzazione

Questa funzione ha la responsabilità del raccordo di FriulAdria con la Capogruppo in materia di governo, gestione e sviluppo dei sistemi informativi della Banca.

(ii) Ufficio Compliance

In relazione ad attività sensibili di cui sopra, l'ufficio Compliance, promuoverà tavoli di confronto con i referenti D.lgs 31 della Capogruppo con l'obiettivo di condividere le misure di sicurezza, tecnologiche ed organizzative, da adottare o già in essere per garantire la conformità del modello di FriulAdria (art. 24 bis).

4. PRINCIPI E REGOLE DI COMPORTAMENTO

4.1. Regole generali di comportamento

Per ciascuna delle Attività Sensibili di cui alla presente Parte Speciale sono previste specifiche procedure in forza delle quali siano garantiti i seguenti requisiti:

- i software e le banche dati installati sui sistemi informativi della Banca siano sempre muniti di valida licenza di utilizzo;
- la rete informatica della Banca ed i dati presenti nella stessa siano preservati da accessi ed utilizzi impropri;
- sia fornito accesso da e verso l'esterno a mezzo di connessione internet esclusivamente ai sistemi informatici dei soggetti che ne abbiano effettiva necessità ai fini lavorativi;
- sia accertato da parte della funzione competente che tutte le opere dell'ingegno utilizzate dalla Banca sotto qualsiasi forma (trasmissione sulla web tv, eventi aperti al pubblico, pubblicazioni proprie, corsi di elearning ecc.), siano sempre utilizzate in conformità alle disposizioni in materia di diritto d'autore;
- il personale ritenuto esposto al rischio di commissione dei reati in materia di diritto d'autore sia sempre adeguatamente formato e sensibilizzato a tenere comportamenti corretti.

Sulla base di tali principi, la presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 - *novies* del D.Lgs. 231/2001);
- detenere programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE);
- mettere a disposizione di terzi, riprodurre, divulgare, trasmettere o diffondere, in tutto o in parte, opere dell'ingegno tutelate dal diritto d'autore e dai diritti connessi;
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

- installare sui sistemi informativi della Banca programmi per elaboratore non assistiti da valida licenza d'utilizzo;
- installare sui sistemi informatici della Banca software (c.d. P2P, di files sharing o instant messaging) mediante i quali è possibile scambiare con altri soggetti all'interno della rete internet ogni tipologia di files, quali filmati, documenti, canzoni, opere letterarie;
- scaricare sui personal computer della Banca programmi prelevati da internet o da sistemi *peer to peer*, anche qualora trattasi di software gratuiti (freeware) o shareware, salvo espressa autorizzazione del Responsabile della Sicurezza dei Sistemi Informativi (RSSI);
- installare sui personal computer della Banca apparati di comunicazione propri (ad esempio modem);
- ascoltare sui personal computer della Banca files audio o musicali, nonché visionare video e/o immagini, su qualsiasi supporto essi siano memorizzati, se non a fini prettamente lavorativi.

I Destinatari debbono pertanto:

1. utilizzare esclusivamente i software, le applicazioni, i files e le apparecchiature informatiche fornite dalla Banca e farlo esclusivamente per finalità strettamente attinenti allo svolgimento delle proprie mansioni;

2. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informatici ed ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Banca;
3. rispettare le policy interne in merito ai dispositivi antintrusione e antivirus;
4. custodire le password di accesso alla rete aziendale ed alle diverse applicazioni e le chiavi personali secondo criteri idonei a impedirne una facile individuazione ed un uso improprio;
5. non prestare o permettere a terzi l'uso delle apparecchiature informatiche della Banca o dell'archivio informatico della stessa, senza la preventiva autorizzazione del Responsabile della Sicurezza dei Sistemi Informativi (RSSI);
6. astenersi dall'effettuare copie non specificamente autorizzate dal Responsabile della Sicurezza dei Sistemi Informativi (RSSI) di dati e di software di proprietà della Banca;
7. evitare di trasferire all'esterno della Banca e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Banca stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
8. qualora per la connessione alla rete internet si utilizzino collegamenti *wireless*, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Banca, possano illecitamente collegarsi alla rete internet tramite i *routers* della stessa e compiere illeciti ascrivibili ai dipendenti;
9. utilizzare opere dell'ingegno senza l'autorizzazione del soggetto che legittimamente ne detiene i diritti, ovvero senza aver stipulato un valido contratto di licenza.

Per ciascuna delle operazioni di carattere significativo individuate nella presente Parte Speciale sono previste specifiche procedure in forza delle quali:

- a) sia previsto (compatibilmente con la normativa vigente in materia di diritto del lavoro e di diritto alla privacy) il costante monitoraggio della rete informatica interna;
- b) siano adottati adeguati programmi di formazione del personale ritenuto esposto al rischio relativo ai reati di cui alla presente Parte Speciale e sia attuata una politica di sensibilizzazione di tutti gli utenti alla sicurezza informatica;
- c) la rete informatica della Banca sia dotata di adeguate protezioni, così da evitare la non corretta duplicazione, riproduzione, trasmissione o divulgazione di opere dell'ingegno protette, ed in particolare delle opere letterarie nella disponibilità della Banca;
- d) sia prevista l'attuazione di un tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici contenuti nel sistema informativo della Banca;
- e) sia assicurato che tutti i supporti informatici alienati o smaltiti (personal computer, floppy disc, CD o DVD) siano resi illeggibili prima della loro vendita o distruzione, così da evitare l'involontaria diffusione di programmi e/o contenuti protetti;
- f) sia previsto che la funzione competente, prima di utilizzare per l'attività della Banca un'opera coperta da diritto d'autore, si accerti di averne pieno titolo;
- g) nel caso di collaborazione con agenzie di comunicazione, di pubblicità ecc., sia con le stesse contrattualizzato che tutti gli adempimenti concernenti il diritto d'autore relativi all'oggetto della prestazione sono stati adempiuti da tali soggetti, che si impegnano a tenere indenne la Banca da qualsiasi pretesa che venisse alla stessa rivolta a tale riguardo;
- h) in caso di evento aperto al pubblico, sia corrisposto in favore della Società italiana degli autori ed editori (SIAE) il compenso di legge, ove lo stesso risulti dovuto.

4.2. Regole specifiche di comportamento

Installazione ed utilizzo dei programmi per elaboratore

La Banca adotta una procedura che assicura che su tutti i sistemi informativi in uso vengano installati esclusivamente programmi per elaboratore muniti di valida licenza di utilizzo ed approvati dalla Banca.

In particolare, detta procedura prevede che:

- sia previsto un sistema di privilegi tale per cui l'installazione di nuovi software o applicazioni sia riservata esclusivamente ai soggetti all'uopo individuati dalla Banca (ai fini del presente documento e salvo diversa definizione nelle specifiche procedure i c.d. "amministratori di sistema");
- sia redatta una policy a cui gli amministratori di sistema dovranno attenersi;
- l'attività posta in essere dagli amministratori di sistema sia tracciabile;
- sia impedito - anche eventualmente inibendo la funzionalità delle porte usb e delle unità CD ROM dei terminali - agli utenti differenti dagli amministratori di sistema di installare software o applicazioni, con la sola esclusione dei soggetti espressamente individuati dalla funzione aziendale competente per ragioni interenti all'attività lavorativa svolta;
- siano utilizzati dalla Banca sistemi antivirus (attualmente, è in uso l'agente antivirus "Sophos") e firewall che blocchino il download dal web di software ed applicazioni non autorizzate;
- la Banca verifichi con cadenza puntuale e periodica la corrispondenza delle licenze in essere con il numero di terminali nella sua disponibilità.

Acquisto di nuove licenze

La Banca adotta una procedura volta a formalizzare l'acquisto di nuove licenze informatiche con i seguenti contenuti:

- la funzione aziendale che rileva la necessità di acquistare un nuovo software o applicativo predispona un progetto esplicativo e ne chiede l'approvazione;
- il progetto viene sottoposto all'approvazione del comitato competente a seconda dell'oggetto, del livello di spesa e della durata dell'impegno;
- il comitato competente concede l'autorizzazione, abilitando il servizio di spesa;
- l'ufficio acquisti effettua il relativo ordine;
- l'installazione dei nuovi software o applicativi viene effettuata dagli amministratori di sistema del settore di competenza;
- il processo autorizzativo di cui sopra viene formalizzato per iscritto.

Utilizzo da parte della Banca di opere coperte da diritto d'autore

La Banca adotta una procedura avente i seguenti contenuti per tutti i casi in cui la stessa sotto qualsiasi forma (trasmissione sulla web tv, eventi aperti al pubblico, pubblicazioni proprie, corsi di elearning ecc.), utilizza opere dell'ingegno protette dal diritto d'autore:

- la funzione competente, prima di utilizzare per l'attività della Banca un'opera o parte di essa coperta da diritto d'autore, si accerti di averne pieno titolo;

- la funzione competente tenga traccia scritta dell'attività di verifica di cui al punto che precede e delle sue risultanze, conservando l'eventuale documentazione rilevante (ad esempio contratti, liberatorie, dichiarazioni di terzi ecc.);
- nel caso di utilizzo da parte della Banca di agenzie di comunicazione, di pubblicità ecc. per attività che coinvolgono opere protette da diritto d'autore, sia con le stesse contrattualizzato che tutti gli adempimenti concernenti il diritto d'autore relativi all'oggetto della prestazione sono stati adempiuti da tali soggetti, i quali si impegnano a tenere indenne la Banca da qualsiasi pretesa che venisse alla stessa rivolta a tale riguardo da terzi;
- nel caso di intervento di artisti alle iniziative organizzate dalla Banca, sia ottenuta la loro autorizzazione scritta alla trasmissione dell'evento (ove prevista) e siano contrattualizzati con i medesimi le modalità della loro prestazione, gli eventuali limiti allo sfruttamento dell'immagine ed i relativi diritti economici.

4.5 Policy e procedure specifiche

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, Codici di Comportamento, *policy* e procedure del Gruppo e di FriulAdria come di seguito indicati.

Tali *policy* e procedure e loro eventuali successive integrazioni o modifiche si considerano parte integrante del Modello di Organizzazione e Controllo della Banca e, pertanto, si devono intendere come recepite nella loro configurazione.

A tal riguardo, si elencano i documenti quelli maggiormente rilevanti:

- (a) Codice Etico/Codice di Comportamento Interno;
- (b) *Policy active directory*

Le *policy* e procedure sono rinvenibili, nella loro versione aggiornata, nell'intranet aziendale.

5. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, ove nell'ambito dei propri controlli periodici lo stesso ravvisi l'esistenza di Attività Sensibili con riferimento ai reati presupposto di cui alla presente Parte Speciale, si attiverà per adeguare la presente Parte Speciale e completarla i principi procedurali ritenuti necessari.