

COIMA SGR S.p.A. –

Società di Gestione del Risparmio

MODELLO DI ORGANIZZAZIONE E GESTIONE

AI SENSI DEL DECRETO LEGISLATIVO

8 GIUGNO 2001, N. 231

PARTE SPECIALE “H”

DELITTI IN VIOLAZIONE DEL DIRITTO D’AUTORE

PARTE SPECIALE “H” – DELITTI IN VIOLAZIONE DEL DIRITTO D’AUTORE

1. Le “attività sensibili” ai fini del D.lgs. n. 231/2001

L’art. 6, comma 2, lett. a) del D.lgs. n. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal decreto, l’individuazione delle cosiddette attività “sensibili” o “a rischio”, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.lgs. n. 231/2001.

Il nucleo delle ipotesi di reato, oggetto della presente Parte Speciale, si rinviene in attività consistenti nella violazione del diritto d’autore protetto dalla Legge n. 633/1941; in particolare tale legge protegge:

- le opere dell’ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all’architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione;
- i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con l. 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell’autore.

In dettaglio, la protezione, per quanto possa interessare ai fini della presente Parte Speciale, comprende *inter alia*:

- i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell’autore;
- le banche di dati intese come “raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo”;
- qualsivoglia immagine, fotografia, contenuto multimediale, elaborato, scritto appartenente a terzi.

Alla luce di quanto appena descritto, l’analisi dei processi aziendali di COIMA SGR S.p.a. (“COIMA SGR”), ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall’art. 25-*novies* del D.lgs. n. 231/2001. Qui di seguito sono elencati i processi esaminati unitamente alle attività sensibili identificate al loro interno e le funzioni/unità organizzative coinvolte di COIMA SGR:

1) **Gestione dei software aziendali e delle banche dati licenziati:** l'attività sensibile si riferisce alle modalità attraverso cui COIMA SGR acquisisce e gestisce software e/o banche dati di terzi protetti da licenza.

➤ **Principali Funzioni/Unità Organizzative coinvolte:**

Amministratore Delegato, Finance, Human Resources, Organization, Information & Digital Transformation.

➤ **Reati ipotizzabili:**

- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore (art. 171-bis, c.1 l. 633/1941);
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in 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, c. 2, l. 633/1941)

2. Il sistema dei controlli

Il sistema dei controlli, perfezionato da COIMA SGR sulla base delle indicazioni fornite dalle principali associazioni di categoria, quali le Linee guida Confindustria, prevede con riferimento alle attività sensibili e ai processi strumentali individuati:

- principi generali di comportamento relativi alle attività sensibili;
- protocolli di controllo “specifici” applicati alle singole attività sensibili.

I protocolli di controllo sono fondati sulle seguenti regole generali, che devono essere rispettate nell'ambito di ogni attività sensibile individuata:

- **Segregazione dei compiti:** preventiva ed equilibrata distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi, idonei ad evitare commistione di ruoli potenzialmente incompatibili o eccessive concentrazioni di responsabilità e poteri in capo a singoli soggetti. In particolare, deve essere garantita la separazione delle attività e responsabilità tra chi autorizza, chi esegue e chi controlla una determinata operazione nelle attività sensibili. In particolare, deve essere garantita la separazione delle attività e responsabilità tra chi autorizza, chi esegue e chi controlla una determinata operazione nelle attività sensibili.
- **Norme:** esistenza di disposizioni aziendali e/o di procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Poteri autorizzativi e di firma:** i poteri autorizzativi e di firma devono essere:

- i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese;
- ii) chiaramente definiti e conosciuti all'interno di COIMA SGR.

- **Tracciabilità:**

- i. ogni operazione relativa all'attività sensibile deve essere, ove possibile, adeguatamente registrata;
- ii. il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali;
- iii. in ogni caso, deve essere disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

2.1 Principi generali di comportamento prescritti nelle attività sensibili

Divieti

La presente Parte Speciale prevede l'espresso divieto - a carico degli Esponenti Aziendali, in via diretta, ed a carico dei Collaboratori esterni, fornitori e professionisti, tramite apposite clausole contrattuali di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-novies del D.lgs. 231/2001);
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

In particolare, è fatto divieto di:

- effettuare il download di qualsivoglia applicazione da Internet, sia da parte di personale interno sia da parte di soggetti esterni, che si collegano mediante il sistema telematico di COIMA SGR;
- utilizzare banche dati, software in assenza di contratto di licenza;
- produrre, distribuire o cedere a terzi i contenuti delle banche dati;
- duplicare software, programmi ed altre opere dell'ingegno coperti da licenze;
- duplicare abusivamente, importare, distribuire, vendere, detenere, installare, concedere in locazione programmi per elaboratore contenuti in supporti non contrassegnati SIAE;
- riprodurre, trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico illegittimamente il contenuto di una banca dati, ovvero estrarre o reimpiegare illegittimamente distribuire, installare, vendere, concedere in locazione la stessa o i dati ivi contenuti.

	MODELLO DI ORGANIZZAZIONE E GESTIONE	Revisione 12 Pagina 5 di 6
---	---	--

- pubblicare un'opera dell'ingegno protetta, o parte di essa, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, senza il consenso del titolare.

Doveri

La presente sezione prevede l'espresso obbligo a carico dei soggetti sopra indicati di:

- acquistare, realizzare, mettere in rete unicamente contenuti (fotografie, sequenze video, commenti, recensioni, articoli e altri contenuti scritti) con licenza d'uso o comunque in regola con la normativa in materia di diritto d'autore e degli altri diritti connessi al loro utilizzo;
- verificare (ad opera di uno o più responsabili a ciò espressamente delegati) preventivamente, ove possibile, o mediante specifica attività di controllo anche periodica, con il massimo rigore e tempestività, che i contenuti in rete siano conformi alle normative vigenti in materia di diritto d'autore e diritti connessi all'utilizzo delle opere dell'ingegno protette;
- verificare che per tutti i contenuti di cui sopra che vengano immessi in rete ad opera di terzi o acquistati da COIMA SGR e immessi in rete, vi sia espressa assunzione di responsabilità da parte dei terzi medesimi in ordine al rispetto delle norme in materia di diritto d'autore e degli altri diritti connessi all'utilizzo delle opere dell'ingegno;
- verificare che l'immissione in rete di tutti i predetti contenuti da parte degli utenti avvenga previa identificazione (registrazione e autenticazione) degli utenti medesimi e espressa assunzione di responsabilità da parte di questi ultimi in ordine all'immissione in rete di contenuti protetti dalle norme in materia di diritto d'autore e degli altri diritti connessi al loro utilizzo;
- utilizzare solo software con licenza d'uso e nei limiti ed alle condizioni previste dalla normativa vigente e dalla licenza medesima, ad eccezione di quei programmi per elaboratore disponibili per il download e utilizzo libero, sempre alle condizioni e nei limiti previsti dalla legge o dal titolare del diritto d'autore e degli altri diritti connessi al suo utilizzo;
- utilizzare solo banche dati con licenza d'uso e nei limiti ed alle condizioni previste dalla normativa vigente e dalla licenza medesima ad eccezione di quelle liberamente consultabili, sempre alle condizioni e nei limiti previsti dalla legge o dal titolare del diritto d'autore e degli altri diritti connessi al suo utilizzo, anche per quanto attiene alla ricerca, estrazione, elaborazione, rielaborazione e pubblicazione dei dati ivi contenuti.

È inoltre tassativamente imposto di assicurare un pieno rispetto della legge n. 633/1941.

Le condotte di ordine generale sopra descritte integrano e non sostituiscono i principi previsti dal Codice Etico, nonché le eventuali procedure di maggiore tutela previste dal Manuale delle Procedure Organizzative di COIMA SGR, che si considera ivi integralmente richiamato.

Si rendono, altresì, applicabili le disposizioni previste dalla Parte Speciale G – Reati informatici e di trattamento illecito di dati.

2.2 Standard di controllo specifici

Qui di seguito sono elencati i protocolli di controllo specifici relativi alle singole attività sensibili individuate:

1) Gestione dei software aziendali e delle banche dati licenziati

Con riferimento a tale area sensibile è necessario seguire tali protocolli:

- definire con chiarezza ruoli e compiti delle Funzioni della gestione delle varie fasi del processo sensibile ed, in particolare, (i) della selezione degli applicativi e delle banche dati necessarie per lo svolgimento dell'attività aziendale; (ii) della stipulazione dei contratti di licenza; (iii) del controllo e della verifica dell'esistenza e della vigenza delle licenze;
- prevedere: i) modalità per acquisto di software e banche dati protetti da licenze; ii) modalità per l'installazione e utilizzo di software e banche dati protetti da licenze; iii) monitoraggio in merito al corretto utilizzo di software e banche dati protetti da licenze.
- predisporre periodicamente una lista dei software e banche dati protetti da licenza e metterla a disposizione dell'Organismo di Vigilanza.

A tal fine è necessario il rispetto delle procedure relative alla gestione informatica richiamante nella Parte Speciale G – Reati informatici, e “Procedura di gestione delle risorse umane”, “Procedura di approvvigionamento e selezione dei fornitori”, predisposte ed attuate in coerenza con i protocolli di cui sopra.