SOGESID S.P.A

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE – "I"

REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO

Rev. VI

DOCUMENTO APPROVATO DAL CONSIGLIO DI AMMINISTRAZIONE IN DATA 18/02/2021

INDICE

- PARTE SPECIALE "I"-

1. REATI APPLICABILI ALLA SOCIETÀ

Per quanto concerne la presente Parte Speciale "I", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell'art. 25-novies del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili dalla Società, in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs.231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state realizzate anche attraverso le interviste ai soggetti aziendali di ciascuna Direzione/Unità Organizzativa competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

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, legge n. 633/1941 comma 1 lett. a) bis)

Il reato punisce chiunque che, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un´opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all´estero contrariamente alla legge italiana; a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un´opera dell´ingegno protetta, o parte di essa; b) rappresenta, esegue o recita in pubblico o diffonde, con o senza variazioni od aggiunte, un´opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell´opera cinematografica, l´esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico; c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge; d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di riprodurre o di rappresentare.

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 legge n.633/1941 comma 1)

È punito chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE).

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 legge n. 633/1941)

È punito chiunque a fini di lucro: a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un´opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati(…).

2. ATTIVITÀ SENSIBILI

Le attività che la Società ha individuato come sensibili, nell'ambito dei delitti in materia di violazione del diritto d'autore, sono indicate in dettaglio nella "Matrice delle Attività a Rischio-Reato", conservata a cura della Società.
Le aree di attività ritenute più specificamente a rischio ai fini della presente Parte speciale "I", sono di seguito riepilogate sulla base della numerazione indicata all'interno della "Matrice delle aree a rischio-reato ex D.Lgs. 231/2001".

Si evidenzia che le possibili modalità e finalità di realizzazione delle principali fattispecie di reato connesse alle Aree e alle Attività sensibili sono indicate, a titolo esemplificativo e non esaustivo, nella "Matrice delle aree a rischio-reato ex D.Lgs. 231/2001" allegata al Modello 231.

F. RELAZIONI ESTERNE E COMUNICAZIONE

F.2) Cura e aggiornamento dei contenuti comunicativi e redazionali dei mezzi informativi aziendali (sito istituzionale, Linkedin, ecc.) e rassegna stampa, con particolare attenzione alle attività di:

- verifica e valutazione informazioni da pubblicare;

- circolarizzazione di articoli in materie di interesse aziendale.

Principali fattispecie di reato connesse

- Violazione delle norme in materia di protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, comma 1, lettera a) bis e comma 3 L.633/41)
- 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. n. 633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione (Art. 171-ter legge n.633/1941)

Principali Ruoli/Aree coinvolti

- ✓ Presidente e Amministratore Delegato "PAD"
- ✓ Ufficio Relazioni Esterne e Comunicazione

F.3) Gestione eventi e convegni, inclusa l'attività riferita a:

- organizzazione eventi;

- gestione mediatica dell'evento;

- supporto per la partecipazione dell'azienda ad eventi esterni.

Principali fattispecie di reato connesse

- Violazione delle norme in materia di protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, comma 1, lettera a)bis e comma 3 L.633/41)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione (Art. 171-ter legge n.633/1941)

Principali Ruoli/Aree coinvolti

- ✓ Presidente e Amministratore Delegato "PAD"
- ✓ Ufficio Relazioni Esterne e Comunicazione
- ✓ DAPL
- ✓ RUP

O. GESTIONE INFRASTRUTTURE INFORMATICHE

O.2) Implementazione e gestione della sicurezza dei dati informatici

Principali fattispecie di reato connesse

- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, 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 un programma per elaboratori (art. 171-bis, comma 1 Legge 633/41)

Principali Ruoli/Aree coinvolti

- ✓ DAPL
- ✓ Information Technologies - Amm. di sistema

3. PRINCIPI GENERALI DI COMPORTAMENTO

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D. Lgs.231/2001 e del Codice Etico e di Condotta adottato dalla Società, nello svolgimento delle attività sensibili sopra citate, tutti i Destinatari del Modello sono tenuti ad osservare i seguenti principi di comportamento.

In particolare, è fatto divieto ai soggetti destinatari della presente parte speciale di:

- Porre in essere comportamenti tali da integrare le fattispecie di reato previste dall' art. 25-novies del D. Lgs. n. 231/2001 riguardanti i delitti in materia di violazione del diritto d'autore presentati nel capitolo 1 "Reati applicabili alla società" ed identificati nella Matrice delle attività rischio-reato.
- Utilizzare software privi delle necessarie autorizzazioni/ licenze nell'ambito dei sistemi informativi aziendali.
- Duplicare e/o diffondere, in qualsiasi forma, programmi e documenti elettronici non nelle forme e per gli scopi di servizio per i quali sono stati assegnati e senza il rispetto delle licenze ottenute.
- Diffondere e/o trasmettere, attraverso siti internet opere di terzi tutelate dal diritto d'autore in mancanza di accordi con i relativi titolari, o in violazione dei termini e delle condizioni previste in detti accordi.
- Realizzare qualunque condotta finalizzata, in generale, alla duplicazione, di programmi per elaboratore protetti dal diritto d'autore o banche di dati sulla memoria fissa del computer.
- Installare programmi per elaboratore senza aver preventivamente informato la funzione aziendale preposta alla gestione della sicurezza informatica.
- Scaricare dal web e installare programmi o applicazioni coperti dal diritto d'autore e comunque senza adeguata autorizzazione da parte della funzione aziendale preposta alla gestione della sicurezza informatica.
- Riprodurre anche durante l'organizzazione di convegni/eventi programmi e contenuti non contrassegnati/autorizzati dalla Società italiana degli autori ed editori (SIAE).
- Riprodurre o diffondere, in qualunque forma e senza averne autorizzazione/diritto, l'opera intellettuale altrui, in mancanza di accordi contrattuali formalizzati per iscritto con i relativi titolari per lo sfruttamento economico o in violazione dei termini e delle condizioni previste in detti accordi.

4. PRINCIPI DI CONTROLLO SPECIFICI

Al fine di evitare la commissione dei reati di cui alla presente Parte Speciale, la Società ha previsto, con riferimento alle aree a rischio

- Relazioni esterne e comunicazione
- Gestione infrastrutture informatiche

I principi di controllo specifici di seguito elencati.

Relazioni esterne e comunicazione

- Segregazione dei compiti, in particolare tra chi:
  - predispone il Piano di Comunicazione annuale e chi lo approva;
  - verifica la necessità di diffondere un comunicato stampa e chi lo approva;
  - predispone i contenuti informativi da pubblicare sul sito aziendale/social network ufficiale e chi li approva.
- Individuazione di ruoli e responsabilità nella gestione dell'organizzazione di eventi di interesse e di promozione dell'immagine della Società.
- Condivisione del Piano di Comunicazione annuale con tutti i Responsabili di Direzione/Area/Servizio.
- Coordinamento del servizio di rassegna stampa, eventualmente affidato a società esterne, a cura della funzione aziendale preposta.
- Cura dei rapporti con i media e con i comunicatori istituzionali da parte della funzione aziendale preposta.
- Formalizzazione di comunicazioni per iscritto o tramite email, della partecipazione dei rappresentanti aziendali agli eventi in cui è coinvolta la Società.
- Svolgimento di controlli, da parte della funzione aziendale preposta, della effettiva rilevanza/utilità della partecipazione ad un evento da parte di un rappresentante della Società, nonché dell'attinenza delle tematiche trattate nell'ambito dell'evento stesso rispetto all'attività svolta dalla Società.
- Inserimento nei contratti stipulati con i collaboratori/società di comunicazione di specifiche informative sulle norme comportamentali adottate dalla Società relativamente al Modello Organizzativo e al relativo Codice Etico e di Condotta, ai principi comportamentali che ispirano la Società e alle normative vigenti.
- Tenuta dell'Agenda degli incontri con i portatori pubblici di interessi e verifica della completezza delle informazioni fornite a cura della funzione aziendale preposta.

- Dazione o ricezione di omaggi, regali e altre forme di benefici nel rispetto dei limiti previsti dalle procedure aziendali e dal Codice Etico e di Condotta della Società.

Gestione infrastrutture informatiche

- Pianificazione di attività di routine e straordinarie da parte della funzione aziendale preposta mediante la predisposizione del "Piano di attività sistemi informatici".
- Previsione di credenziali di autenticazione e di accessi sugli applicativi aziendali adeguatamente tracciati su log, nel rispetto della normativa vigente.
- Previsione di applicazioni che tengono traccia delle modifiche, compiute dagli utenti, ai dati ed ai sistemi aziendali.
- Definizione di criteri e modalità per l'assegnazione, la modifica e la cancellazione dei profili utente.
- Definizione di meccanismi di monitoraggio del traffico e di tracciabilità degli eventi di sicurezza sulle reti (ad esempio: accessi anomali per frequenza, modalità, temporalità).
- Definizione di una policy formale che regoli le modalità operative per la messa a disposizione e la corretta gestione delle risorse informatiche.
- Formalizzazione, a cura della funzione aziendale preposta, di appositi report al fine di condividere con il Vertice societario la presenza di eventuali anomalie riscontrate e di attività straordinarie svolte.
- Esecuzione quotidiana e automatica di backup dei dati sui server aziendali.
- Verifica del corretto funzionamento dei server aziendali al fine di individuare operazioni anomale o malfunzionamenti e di prevenire accessi non autorizzati sugli apparati informatici aziendali.
- Verifica periodica avente ad oggetto lo stato di aggiornamento delle componenti software di base.
- Verifica periodica avente ad oggetto l'applicazione delle misure minime di sicurezza (ad es. accessi fisici alla sala CED, correttezza delle procedure di archiviazione dei dati trattati, ecc.).
- Aggiornamento e pubblicazione dei dati/informazioni aziendali e manutenzione del sito web aziendale da parte della funzione aziendale preposta previa autorizzazione del Vertice aziendale.
- Gestione del servizio di posta elettronica aziendale, compresa la PEC, secondo le modalità definite nelle apposite procedure interne.

- Divieto d'uso della casella di posta aziendale per finalità estranee alle esigenze di servizio.
- Esecuzione dei backup di file di progetto mediante supporto idoneo, identificabile e rintracciabile, archiviato a cura della funzione aziendale preposta.
- Verifica del materiale informatico acquistato e tempestiva segnalazione di eventuali incongruenze riscontrate.
- Installazione e configurazione di nuovi apparati a cura del personale tecnico specializzato.
- Assegnazione e utilizzo degli strumenti informatici sulla base delle procedure/regolamenti interni.
- Archiviazione della documentazione e delle registrazioni all'interno del Sistema documentale aziendale depositato sui Server.
- Gestione dell'elenco dei dispositivi HW e i SW aziendali da parte delle funzioni aziendali preposte e formalizzazione dello stesso mediante apposita modulistica.
- Esecuzione delle attività di verifica, validazione ed eventuale manutenzione/aggiornamento di SW e formalizzazione delle stesse mediante apposita modulistica.
- Protezione della rete di trasmissione dati aziendale da adeguati strumenti di limitazione degli accessi (firewall e proxy).
- Protezione dei sistemi informativi aziendali mediante programmi antivirus, aggiornati in modo automatico, al fine di evitare il rischio di intrusione.
- Definizione di procedure al fine di rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi.
- Predisposizione di un piano di emergenza in caso di malfunzionamento o di fermo del sistema.
- Garanzia della corretta esecuzione delle operazioni di avvio e chiusura del sistema.
- Valutazioni periodiche al fine di verificare l'adattabilità e l'integrità delle misure di sicurezza.
- Definizione di regole per la navigazione in Internet che includono, in particolare:
    - l'utilizzo della rete al solo fine lavorativo;
    - il divieto di scaricare software nelle strutture informative aziendali;
    - il divieto di connessione a siti segnalati.

Principali procedure operative (PO), istruzioni operative (IST), regolamenti (Reg.) di riferimento:

- PO 01 – Redazione, modifica e tenuta sotto controllo della documentazione e delle registrazioni
- PO 04 – Gestione delle infrastrutture
- PO 13 – Amministrazione trasparente
- PO 14 - Omaggi, regalie ed altre forme di utilità
- PO 16 – Attività di comunicazione
- IST 01 – Archiviazione documentale e protocollo
- IST 7a – Sistemi informativi ed informatici
- IST 7B – Regolamento utilizzo strumenti informatici
- IST 11 – Flusso informativo in materia di trasparenza
- Procedure amministrative contabili del Dirigente Preposto compliance con il D.Lgs. 262 del 2005 – Sistemi informativi