MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

di

SIAE

Società Italiana Autori ed Editori

(ex Decreto Legislativo n. 231/2001)

PARTE SPECIALE B – REATI INFORMATICI, TRATTAMENTO ILLECITO DEI DATI E DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE

Approvato con delibera del Consiglio di Gestione del 20/12/2018

INDICE

1. Le fattispecie dei reati

1.1 Premessa

Ai fini di una migliore comprensione della normativa in materia di responsabilità amministrativa degli enti, di seguito sono descritti, per tratti essenziali, i reati la cui commissione da parte dei soggetti riconducibili alla società può ingenerare responsabilità della società stessa.

La presente Parte Speciale B è dedicata alla trattazione delle attività di gestione ed utilizzo dei sistemi informativi aziendali potenzialmente a rischio o strumentali per la realizzazione dei reati informatici e trattamento illecito dei dati, così come previsti dai reati rilevanti ai sensi dell'art. 24-bis del Decreto, nonché di delitti in materia di violazione del diritto di autore ex art. 25-novies del Decreto.

Nei due paragrafi successivi sono illustrate in dettaglio le fattispecie di reato contemplate nei citati articoli, con l'indicazione (mediante sottolineatura) la cui commissione potenziale è emersa durante l'analisi di SIAE.

Per una trattazione completa delle ipotesi di reato previste dal D.Lgs. 231/2001, comprensiva del testo e di una casistica sintetica, si veda "SIAE – MOGC Parte Generale", allegato 1 "I reati e gli illeciti amministrativi per i quali trova applicazione il D.Lgs. 231/2001".

1.2 I reati di cui all'art. 24-bis del Decreto Legislativo n.231/2001

- Accesso abusivo ad un sistema informatico o telematico (*art 615-ter c.p.*)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (*art. 635-bis c.p.*)
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
- Danneggiamento di sistemi informatici o telematici (*art. 635-quater c.p.*)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (a*rt. 615-quater c.p.*)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
- Falsità in un documento informatico pubblico o privato (*art. 491-bis c.p.*)
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (*art. 640-quinquies c.p.*)

1.3 I reati di cui all'art. 25-novies del Decreto Legislativo n.231/2001

- Violazioni del diritto d'autore. (*artt. 171, co. 1 lett. a bis), co. 3,*, *171-bis, 171-ter, 171-septies, 171-octies L. 633/41).*

2. Funzione della Parte Speciale

Obiettivo della presente Parte Speciale è consentire che i componenti degli Organi Sociali, i Dipendenti, i Consulenti e Mandatari, coinvolti nei Processi Sensibili, mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati indicati nel paragrafo precedente.

Si è già detto nella Parte Generale che il perseguimento delle finalità di prevenzione dei Reati richiede una ricognizione dei meccanismi di funzionamento e di controllo dell'azienda, nonché la verifica dell'adeguatezza dei criteri di attribuzione delle responsabilità all'interno della struttura.

In tal senso, si sono individuati in generale i presidi principali per l'attuazione delle vigenti previsioni normative, costituiti da:

a) Modello di organizzazione, gestione e controllo;

b) Codice Etico;

c) Sistema Sanzionatorio;

d) Sistema di Comunicazione.

Allo stesso modo, sono stati individuati gli elementi caratteristici di ciascun presidio principale ed in particolare:

a) l'istituzione di un Organismo di Vigilanza autonomo ed indipendente cui è affidato il compito di controllare il grado di effettività, adeguatezza, mantenimento ed aggiornamento del Modello, la predisposizione di meccanismi procedurali volti a razionalizzare le fasi di assunzione ed attuazione delle scelte decisionali, in un'ottica di documentabilità e verificabilità delle varie fasi del processo, l'adozione di un sistema chiaro di riparto dei compiti e delle responsabilità, l'operatività di un sistema di flussi informativi tra le diverse strutture aziendali e dalle stesse all'Organismo di Vigilanza, l'adozione di un sistema di *reporting* dell'Organismo di Vigilanza verso gli Organi Sociali, la predisposizione di validi strumenti di controllo (a titolo esemplificativo, schede informative, database dei rischi, criteri di selezione di Dipendenti e dei Mandatari);

b) l'adozione di un Codice Etico che costituisce la carta dei valori della società, debitamente diffuso a tutti i componenti della struttura aziendale, ai Mandatari ed alle controparti contrattuali, costantemente aggiornato e monitorato;

c) l'adozione di un sistema disciplinare volto a garantire efficacia ed effettività alle prescrizioni interne;

d) la predisposizione di un sistema di comunicazione capillare, efficace, dettagliato, completo e costante, attraverso – ad esempio – manuali operativi, piani di formazione del personale, reti intranet, numeri verdi interni.

In questa Parte Speciale sono invece individuati i principi specifici relativi ai Processi Sensibili, in relazione ai reati di cui al paragrafo precedente.

Verranno quindi indicati:

- le aree e/o i processi aziendali definiti "sensibili" ovvero a rischio di specifico reato;
- i principi fondamentali di riferimento in attuazione dei quali dovranno essere adottate le procedure aziendali ai fini della corretta applicazione del Modello;
- i principi di riferimento che dovranno presiedere alle attività di controllo, monitoraggio e verifica dell'Organismo di Vigilanza e dei responsabili delle altre strutture aziendali che con lo stesso cooperano, debitamente regolate in apposite procedure e/o regolamenti interni da adottare ai fini della corretta applicazione del Modello.

3. Processi Sensibili nell'ambito dei reati informatici, trattamento illecito dei dati e delitti in materia di violazione del diritto d'autore

Le fattispecie di reato indicate *sub* par. 1 si applicano, in via potenziale, a tutte le Divisioni / Uffici / Servizi di SIAE (siano essi dipendenti o collaboratori) che, nell'espletamento delle attività di propria competenza, siano coinvolte a qualsiasi titolo nell'ambito delle attività di gestione e utilizzo dei sistemi informativi aziendali al fine di prevenire la commissione delle fattispecie di reato realizzabili previste dai sopraccitati articoli del Decreto.

I processi aziendali di SIAE per i quali emerge un rischio potenziale di commissione di reati in questo ambito sono:

- Servizi Informativi.

Anche se tutti i processi e le strutture aziendali sono potenzialmente coinvolti, data la pervasività nell'uso dei sistemi informatici.

In particolare, in tale ambito di responsabilità della Direzione Information Technology, le aree di attività ritenute più specificamente a rischio, quali sono state individuate in sede di identificazione dei Processi Sensibili (c.d. *as-is analysis,* per la quale si veda il cap. 6 della Parte Generale), sono le seguenti:

1. Gestione degli accessi logici ai dati e ai sistemi;
2. Gestione dei backup;
3. Gestione di software, apparecchiature, dispositivi o programmi informatici (change management);
4. Gestione della sicurezza della rete;
5. Gestione della sicurezza fisica.

4. Ruoli e Responsabilità

I processi relativi alle suddette aree di attività fanno riferimento alle seguenti unità organizzative aziendali:

Direzione Information Technology: che detiene la responsabilità gestionale sul processo e gestisce gli applicativi ed i sistemi per tutta la società.

Tutte le Divisioni / Uffici / Servizi di SIAE (siano essi dipendenti o collaboratori) che, nell'espletamento delle attività di propria competenza, siano coinvolte a qualsiasi titolo nell'ambito delle attività di gestione e utilizzo dei sistemi informativi aziendali al fine di prevenire la commissione delle fattispecie di reato realizzabili previste dai sopraccitati articoli del Decreto.

5. Principi generali di comportamento

Ai fini della Parte Speciale B, sono stati individuati i Principi di Comportamento cui il personale della SIAE (cfr. Cap. 3, "Destinatari", Parte Generale), a qualsiasi titolo coinvolto nelle attività di gestione e utilizzo dei sistemi informativi, deve attenersi.

Pertanto, i destinatari **devono**:

- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- utilizzare gli strumenti aziendali nel rispetto delle procedure e delle policies aziendali definite;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della SIAE e aggiornare periodicamente le password, evitando che terzi soggetti possano venirne a conoscenza;
- utilizzare beni protetti dalla normativa sul diritto d'autore nel rispetto delle regole ivi previste;
- limitare la navigazione in internet e l'utilizzo della posta elettronica attraverso i sistemi informativi aziendali alle sole attività lavorative.

Ciascun Responsabile di Divisione / Ufficio / Servizio, per la propria unità di pertinenza, deve gestire l'abilitazione degli accessi ai siti di enti pubblici o privati che richiedano credenziali di accesso (user-id, password e/o Smart Card).

Il personale della Direzione Information Technology, in base al proprio ruolo ed alla propria responsabilità, **deve**:

- verificare la sicurezza della rete e dei sistemi informativi aziendali e tutelare la sicurezza dei dati;
- identificare le potenziali vulnerabilità nel sistema dei controlli informatici;
- valutare la corretta implementazione tecnica del sistema "deleghe e poteri" aziendale a livello di sistemi informativi ed abilitazioni utente al fine di rendere possibile la corretta segregazione dei compiti;
- garantire, sui diversi applicativi aziendali, l'applicazione delle regole atte ad assicurare l'aggiornamento delle password dei singoli utenti;
- installare a tutti gli utenti esclusivamente software originali, debitamente autorizzati e licenziati;
- monitorare l'infrastruttura tecnologica al fine di garantirne la manutenzione e la sicurezza fisica;
- effettuare le attività di backup e provvedere al corretto mantenimento dei file di log generati dai sistemi;

- garantire la manutenzione software e hardware dei sistemi e un processo di change management segregato;
- vigilare sulla corretta applicazione di tutti gli accorgimenti ritenuti necessari al fine di fronteggiare, nello specifico, i delitti informatici e il trattamento dei dati suggerendo ogni più opportuno adeguamento.

Inoltre, le attività svolte da parte di fornitori terzi in materia di:

- networking;
- gestione applicativi;
- gestione sistemi hardware.

devono rispettare i principi e le regole aziendali, al fine di tutelare la sicurezza dei dati ed il corretto accesso da parte dei soggetti ai sistemi applicativi ed infrastrutturali.

È fatto esplicito **divieto** di:

- utilizzare le risorse informatiche (es. personal computer fissi o portatili, dispositivi di memorizzazione portatile ecc.) assegnate dalla SIAE per finalità diverse da quelle lavorative;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di:
  - acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;
  - danneggiare, distruggere dati contenuti nei suddetti sistemi informativi;
  - utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;
- porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria ai sensi del D.Lgs. 231;
- utilizzare o installare programmi diversi da quelli autorizzati dalla Direzione Information Technology;
- effettuare download illegali o trasmettere a soggetti terzi contenuti protetti dal diritto d'autore;
- utilizzare impropriamente i sistemi per la produzione di smart card (Card Management System) per i titolari delle biglietterie;
- accedere ad aree riservate (quali server rooms, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente;
- aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (antivirus, firewall, proxy server, ecc.);

- lasciare il proprio personal computer o altri dispositivi di memorizzazione portatile incustoditi e senza protezione;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- utilizzare in modo improprio gli strumenti di firma digitale assegnati;
- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico della Pubblica Amministrazione, al fine di procurare un vantaggio per SIAE;
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato.

Di seguito sono esposti i principi generali di controllo, relativi alle procedure aziendali, volti alla prevenzione dei reati informatici, del trattamento illecito dei dati e dei delitti in materia di violazione del diritto d'autore.

6. Principi di riferimento relativi alle procedure aziendali specifiche

Al fine di fornire la necessaria informativa all'OdV circa l'aderenza alle norme di comportamento sancite dal Modello e le evidenze di funzionalità dei meccanismi di controllo svolte, le strutture coinvolte nelle singole aree di rischio garantiranno la documentabilità (comprovante il rispetto della normativa e delle regole di comportamento e di controllo previste dal Modello) dei processi seguiti, fornendo all'Organismo di Vigilanza la documentazione necessaria.

Le Unità Organizzative coinvolte nella gestione delle attività potenzialmente a rischio sono tenute a fornire adeguata comunicazione all'Organismo di Vigilanza secondo le modalità e le tempistiche indicate nel documento di regolamentazione dei "Flussi informativi verso l'Organismo di Vigilanza.

In questa sezione si riportano i principi di controllo volti a prevenire i comportamenti illeciti previsti dagli artt., 24-bis e 25 novies del D.Lgs. 231/2001.

Le modalità operative per la gestione delle attività in oggetto sono disciplinate anche nei seguenti documenti:

- Documento Programmatico sulla Sicurezza;
- Codice Etico;
- Information Security Policy;
- Specific Security Policy - Classificazione delle Informazioni;
- Specific Security Policy - Controllo degli accessi;
- Specific Security Policy - Gestione dei supporti rimovibili.

Inoltre ai fini dell'adeguamento al Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR) la SIAE, in qualità di Titolare del trattamento, ha i) definito un suo standard di comportamento, formalizzato in apposite Policy aziendali, ii) ha nominato un Data Protection Officer (DPO) come figura di garanzia e iii) previsto l'organizzazione di appositi corsi di formazione per dipendenti e dirigenti.

I principi di controllo sono di seguito elencati:

- svolgimento periodico di attività di valutazione dei rischi nell'ambito della gestione dei sistemi informativi;
- l'attivazione, la modifica o la cessazione di un profilo utente sono autorizzate da parte del Responsabile di Divisione/ Ufficio / Servizio;
- verifica periodica, da parte di ciascun Responsabile di Divisione / Ufficio / Servizio, delle credenziali utente al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi;
- tutti i dati trattati in azienda sono classificati e il loro accesso è profilato;

- la comunicazione della prima password di accesso ai sistemi informativi avviene in modalità confidenziale ed è cura di ogni dipendente la successiva sostituzione, custodia e non divulgazione;
- la Società ha implementato meccanismi di sicurezza logica, tra cui a titolo esemplificativo e non esaustivo:
  - utilizzo di account e password;
  - accessi profilati alle cartelle di rete;
  - le credenziali di autenticazione ai sistemi informativi sono gestite con criteri equipollenti a quanto previsto dal D.Lgs. 196/2003 e s.m.i. (tra cui la previsione di vincoli di sicurezza alfanumerici della password, politiche di rinnovo periodico delle password, ecc.);
- L'accesso ai sistemi informativi avviene tramite autenticazione univoca dell'utente;
- Gli indirizzi di posta elettronica di cui sono dotati i dipendenti sono nominativi e a esclusivo uso lavorativo;
- l'accesso ai sistemi per la produzione di smart card è consentito ad un gruppo limitato di dipendenti appartenenti alla Funzione CMS (Card Management System);
- la protezione contro potenziali attacchi esterni di tutti i server e le *workstations* della SIAE (postazioni fisse e portatili) è garantita attraverso l'utilizzo di software antivirus (aggiornato in modo automatico, che effettua controlli in entrata e in uscita);
- protezione contro potenziali attacchi esterni attraverso l'utilizzo di firewall, IPS e segregazione delle reti.
- gli asset IT (desktop, portatili, ecc.), sono oggetto di censimento e sono dotati di un responsabile di riferimento;
- la Direzione Information Technology effettua tutti gli aggiornamenti dei sistemi operativi e degli applicativi suggeriti dai produttori al fine di limitare i possibili rischi legati a vulnerabilità riscontrate negli stessi;
- la SIAE rilascia certificati elettronici e di firma digitale aventi validità esclusiva per i sistemi di biglietterie automatizzate;
- solamente il personale della Direzione Information Technology è autorizzato ad installare software sulle postazioni di lavoro dei dipendenti;
- tutti i programmi installati sulle postazioni di lavoro sono dotati di licenza;
- il personale della Direzione Information Technology effettua il controllo dei software installati sulle postazioni di lavoro dei dipendenti attraverso un sistema di *sw inventory* della macchina (LAN Desk);

- il personale della Direzione Information Technology effettua una verifica annuale dei software presenti sulle postazioni dei vari utenti, rimuovendo i software vietati o privi di licenza;
- sono effettuati controlli periodici dei software installati sui server;
- la Direzione Information Technology definisce dei piani di backup periodici dei dati, file, programmi e sistemi operativi, al fine di garantire la salvaguardia del patrimonio informativo;
- i backup sono opportunamente conservati e sono eseguiti i relativi test di restore allo scopo di verificare l'integrità dei dati archiviati;
- sono predisposti specifici ambienti di sviluppo e test fisicamente e/o logicamente separati dall'ambiente di produzione;
- solamente le persone autorizzate possono rilasciare aggiornamenti hardware e software in ambiente di produzione;
- quando necessario (ad esempio, quando sono richieste modifiche funzionali) è previsto il coinvolgimento dell'utente nelle attività di test;
- sono previste delle regole di gestione e monitoraggio dei log relativi alla tracciatura degli accessi ai sistemi e alle informazioni critiche, con particolare riferimento alle attività degli amministratori di sistema;
- l'accesso ad internet è regolamentato e risulta essere filtrato da un sistema di web filtering;
- l'accesso tramite VPN è consentito, tramite USB *internet key* e/o *token*, al solo personale abilitato e opportunamente identificato;
- esecuzione di attività di monitoraggio sugli apparati di rete;
- esecuzione peridica di attività di *vulnerability assessment* e *penetration test*;
- l'accesso al Data Center è consentito tramite badge al solo personale autorizzato.
- sono presenti procedure di abilitazione e disabilitazione dei badge per l'accesso al Data Center;
- esecuzione di controlli periodici del personale autorizzato ad accedere alle aree tecniche e al Data Center;
- Il server dedicato alla Funzione CMS per i servizi di biglietteria automatizzata è ubicato in un locale diverso dal Data Center;
- L'accesso al locale CMS è consentito tramite badge al solo personale autorizzato;

- l'accesso alle aree riservate di siti di enti pubblici o privati è consentito solo a personale preventivamente autorizzato (tramite nome utente e password, token di autenticazione e smart card).

7. I controlli dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli a campione, diretti a verificare la corretta esplicazione delle attività connesse ai Processi Sensibili relativi ai reati informatici, al trattamento illecito dei dati ed ai delitti i materia di violazione del diritto d'autore, anche in relazione ai principi espressi nel presente documento (esistenza e adeguatezza della procura, limiti di spesa, regolare effettuazione del *reporting* verso gli organi deputati, ecc.) e, in particolare, alle procedure interne in essere.

A tal fine, si ribadisce che all'Organismo di Vigilanza deve essere garantito, da parte di tutta la struttura della SIAE, libero accesso a tutta la documentazione aziendale rilevante.

Di detti controlli l'Organismo di Vigilanza riferisce al Consiglio di Gestione ed al Direttore Generale.