SIAE DALLA PARTE DI CHI CREA

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

di SIAE

Società Italiana Autori ed Editori
(ex Decreto Legislativo n. 231/2001)

PARTE SPECIALE B
REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

di

SIAE

Società Italiana Autori ed Editori

(ex Decreto Legislativo n. 231/2001)

PARTE SPECIALE B – REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

INDICE

1.Le fattispecie dei Reati

1.1 Premessa

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 di dati, così come individuati dai Reati rilevanti ai sensi dell'art. 24-*bis* del D. Lgs. 231/2001.

Nei due paragrafi successivi sono illustrate le fattispecie di Reato contemplate nei citati articoli, che sono state ritenute astrattamente configurabili in considerazione di alcuni Processi Sensibili svolti dalla Società.

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.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* 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.);
- Falsità in un documento informatico pubblico o privato (art. 491-*bis* c.p.).

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".

2. Funzione della Parte Speciale

Obiettivo della presente Parte Speciale è garantire che i Soggetti Apicali e i Soggetti Sottoposti coinvolti, a qualsiasi titolo, 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.

In questa Parte Speciale sono quindi individuati:

- i Macro Processi e i Processi Sensibili in relazione ai Reati di cui al paragrafo precedente;
- i principi generali di comportamento che devono essere osservati da tutti i Soggetti Apicali e i Soggetti Sottoposti che a qualsiasi titolo intervengo nella gestione del Processo Sensibile;
- i Presidi di Controllo preventivi che devono essere recepiti nelle Procedure e che devono presiedere le attività di monitoraggio e verifica dell'Organismo di Vigilanza.

3. Macro-Processi e Processi Sensibili nell'ambito dei Reati informatici e trattamento illecito di dati

Le fattispecie di Reato indicate *sub.* par. 1 si applicano ai seguenti Macro Processi, per i quali emerge un rischio potenziale di commissione dei suddetti Reati:

- Gestire l'Information Technology;
- Gestire la Governance, Risk e Compliance.

Si evidenzia che le fattispecie di Reato in esame si applicano, in via potenziale, a tutte le Divisioni/Uffici/Servizi della Società (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. Pertanto, tutti i processi e le strutture aziendali si devono ritenere potenzialmente coinvolti, data la pervasività nell'uso dei sistemi informatici.

In particolare, in sede di attività c.d. *as-is analysis* (per la quale si veda il par. 1.5 della Parte Generale), in riferimento a ciascun Macro Processo, sono stati individuati i seguenti Processi Sensibili:

Gestire l'Information Technology:

- Installazione, manutenzione, aggiornamento o gestione di software di soggetti pubblici o forniti da terzi per conto dei soggetti pubblici;
- Gestire gli accessi logici ai dati e ai sistemi;
- Gestire i *backup*;
- Gestire la sicurezza della rete;
- Gestire i SW, apparecchiature, dispositivi o programmi informatici (*change management*);
- Gestire la sicurezza fisica.

Gestire la Governance, Risk e Compliance:

- Gestire gli adempimenti in ambito Reg. (UE) 2016/679.

4. Ruoli e responsabilità[1]

I Processi Sensibili, per come identificati al precedente paragrafo, fanno riferimento alle seguenti entità aziendali, identificate quali Owner del Processo:

Direttore Generale: in relazione a tutte le attività nell'esercizio dei propri compiti;

Presidente del Consiglio di Gestione: in relazione a tutte le attività nell'esercizio dei propri compiti;

Consiglio di Gestione: in relazione a tutte le attività svolte in rappresentanza dell'ente;

Consiglio di Sorveglianza: in relazione a tutte le attività svolte nell'esercizio delle proprie funzioni;

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 precedentemente indicati del Decreto.

Per un dettaglio circa gli Owner di Processo e delle funzioni che intervengono si rimanda ai Manuali di Processo di riferimento.

Fermo quanto precede, i Presidi di Controllo richiamati nella presente Parte Speciale e in particolare nel paragrafo 6, devono e/o dovranno essere osservati dagli Owner di Processo di volta in volta competenti tenuto conto delle modifiche organizzative eventualmente configurabili[2].

[1] Si specifica che le Funzioni richiamate nella presente Parte Speciale sono stati identificati dall'organigramma attualmente vigente.
[2] A tal riguardo, si rimanda all'organigramma vigente.

5. Principi generali di comportamento

Ai fini della Parte Speciale B, sono stati individuati i Principi di Comportamento cui i Destinatari a qualsiasi titolo coinvolto nei Processi Sensibili devono attenersi.

Pertanto, i Destinatari nell'ambito dell'attività di controllo loro attribuita istituzionalmente *ex lege*, **devono**:

- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- utilizzare gli strumenti aziendali nel rispetto delle Procedure interne predefinite;
- 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.

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. 231/2001;
- 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.

6. Presidi di Controllo

(OMISSIS)

6.1 Installazione, manutenzione, aggiornamento o gestione di software di soggetti pubblici o forniti da terzi per conto dei soggetti pubblici

Le Procedure devono essere caratterizzate dalla presenza dei seguenti Presidi di Controllo:

(OMISSIS)

6.2 Gestire gli accessi logici ai dati e ai sistemi

(OMISSIS)

6.3 Gestire i backup

Le Procedure devono essere caratterizzate dalla presenza dei seguenti Presidi di Controllo:

(OMISSIS)

6.4 Gestire la sicurezza della rete

Le Procedure devono essere caratterizzate dalla presenza dei seguenti Presidi di Controllo:

(OMISSIS)

6.5 Gestire i SW, apparecchiature, dispositivi o programmi informatici (*change management*)

Le Procedure devono essere caratterizzate dalla presenza dei seguenti Presidi di Controllo:

(OMISSIS)

6.6 Gestire la sicurezza fisica

Le Procedure devono essere caratterizzate dalla presenza dei seguenti Presidi di Controllo:

(OMISSIS)

6.7 Gestire gli adempimenti in ambito Reg. (UE) 2016/679

Le Procedure devono essere caratterizzate dalla presenza dei seguenti Presidi di Controllo:

(OMISSIS)

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, esso effettua periodicamente controlli a campione, diretti a verificare la corretta esplicazione delle attività connesse ai Processi Sensibili relativi ai Reati informatici e trattamento illecito di dati, 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 in essere.

A tal fine, si ribadisce che all'OdV 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 e al Direttore Generale.