AMAP SPA

Modello Organizzativo ex 231/01

Procedura PO INF – MONITORAGGIO OPERATIVO REATI DA DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

INDICE

	UNITÀ ORGANIZZATIVA	Firma
Redatto da	Dott. Davide La Morella	
Verificato da	Ing. Santi Monasteri	
Approvato da	Amministratore Unico	

Pubblicazione	20/06/2019

Revisione

Revisione	Data	Descrizione
00	24/05/2016	Prima Emissione
01	19/11/2018	Modifica par. 4 e par. 7

1 SINTESI E SCOPO

La presente procedura disciplina gli aspetti inerenti la gestione ed il controllo delle attività aziendali che possono portare alla commissione dei reati cosiddetti "informatici", previsti dall'art 24-bis del Dlgs 231/01 e dall'art. 25-novies del Dlgs 231/01, derivanti dall'utilizzo improprio dei sistemi informativi all'interno dell'AMAP S.p.A. Inoltre, in osservanza del Decreto Legislativo n.231 dell'8 giugno 2001 e norme collegate in tema di responsabilità amministrativa degli enti, la presente procedura costituisce parte integrante del Modello di Organizzazione, Gestione e Controllo dell'AMAP S.p.A. La procedura assolve, fra le diverse finalità, il compito di agevolare il monitoraggio dell'applicazione del Modello di Organizzazione Gestione e Controllo da parte dell'Organismo di Vigilanza e di prevenire la commissione, da parte dei soggetti indicati all'art 5 c 1 Dlgs 231/01 dei seguenti reati:

Art. 24 bis D.L.gs 231/2001 "Delitti Informatici e trattamento illecito dei dati"

- ✓ Art. 635- bis c.p. "Danneggiamento di informazioni, dati e programmi informatici"
- ✓ Art. 635- quater c.p. "Danneggiamento dei sistemi informatici o telematici"

Art. 25 novies D.L.gs 231/2001 "Reati in materia di diritti d'autore"

- ✓ Art. 171 Bis Violazione dei Diritti d'Autore mediante duplicazione di programmi"

2 CAMPO DI APPLICAZIONE

La presente procedura per i reati relativi ai delitti informatici si applica alle attività operative svolte all'interno di AMAP S.p.A che presuppongono l'utilizzo di strumenti informatici sia hardware che software.

3 DEFINIZIONI

Danneggiamento (*vedi art. 635 del Codice Penale*)**:** Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili;

Trattamento: qualunque Operazione o complesso di operazioni concernenti un utilizzo qualsiasi (raccolta, registrazione, conservazione, distruzione etc.) di dati, anche se non registrati in Banca Dati;

Dato Personale: Qualunque informazione, diretta o indiretta, relativa a persona, fisica o giuridica;

Dato Identificativo: i dati personali che permettono l'identificazione diretta dell'interessato;

Banca Dati: Complesso organizzato di dati ripartito in uno o più unità dislocate in uno o più siti;

Reti di comunicazione elettronica: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

Rete pubblica di comunicazioni: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

Servizio di comunicazione elettronica: i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del 7 marzo 2002, del Parlamento europeo e del Consiglio;

Posta elettronica: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;

Misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dal D.lgs 196/2003;

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

Credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

Parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

Profilo di autorizzazione: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

AU: Amministratore Unico

DG: Direttore Generale

COMM: Servizio Commerciale

UC_SINF: Unità Coordinamento Sistemi informatici

4 RESPONSABILITA'

Il presente paragrafo intende correlare, per ciascuna funzione aziendale (Responsabile di Servizio, Responsabile di Unità), lo svolgimento delle attività operative ai possibili reati derivanti da Delitti informatici o dal trattamento illecito dei dati e della violazione dei diritti d'autore previsti dal Dlgs 231/01.

Reati / **Attività**	Art. 635- bis c.p. "Danneggiamento di informazioni, dati e programmi informatici"	Art. 635- quater c.p. "Danneggiamento dei sistemi informatici o telematici"	Art. 171 Bis Violazione dei Diritti d'Autore mediante duplicazione di programmi"
Gestione del sistema informativo aziendale comprensivo di hardware, software e gestione della rete	Tutti	Tutti	Tutti
Installazione di apparecchiature ed hardware	AU, DG, COMM	AU, DG, COMM	

5 CLASSIFICAZIONE DEI RISCHI DI COMMISSIONE DEL REATO

La sottostante tabella riporta l'esito della classificazione del rischio di commissione del reato descritta nel Modello di Organizzazione, Gestione e Controllo per i soggetti responsabili indicati nel paragrafo precedente

Classificazione del rischio / **Reati**	Molto Basso	Basso	Medio	Alto	Molto Alto
Art. 635- bis c.p. "Danneggiamento di informazioni, dati e programmi informatici"			X		
Art. 635- quater c.p. "Danneggiamento dei sistemi informatici o telematici"			X		
Art. 171 Bis Violazione dei Diritti d'Autore mediante duplicazione di programmi"		X			

6 MODALITA' OPERATIVE

6.1. PRINCIPI GENERALI DI COMPORTAMENTO

Uno dei presupposti del Modello al fine i reati "informatici" è dato dal rispetto di alcuni principi e nella tenuta di determinati comportamenti, da parte dei lavoratori della Società, nonché dagli eventuali soggetti esterni che siano coinvolti nelle attività operative che possono esporre l'AMAP S.p.a. al reato presupposto. I principi e lo stile comportamentale sono elencati nel Codice Etico Aziendale.

6.2. ATTIVITÀ SENSIBILI NELL'AMBITO DEI REATI INFORMATICI

Attraverso un'attività di mappatura delle aree a rischio e di controllo, che costituisce parte integrante del Modello, la Società ha individuato le attività sensibili di seguito elencate, nell'ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei reati informatici o i reati relativi ai diritti d'autore:

a. Installazione di apparecchiature per il danneggiamento dei dati contenuti nel sistema informativo aziendale;
b. Danneggiamento volontario di sistemi informatici o telematici.

Va subito sottolineato come la realizzazione dei delitti informatici è di natura dolosa, quindi una violazione volontaria dei soggetti, rispetto ai protocolli operativi.

6.3. PROTOCOLLI DI PREVENZIONE

L'AMAP S.p.A. ha all'interno del proprio sistema di gestione integrato due documenti inerenti la corretta gestione del sistema informativo:

- Procedura Operativa 9.p "Gestione dei Sistemi Informatici"
- Istruzione Operativa 9.p.1 "Gestione backup banche dati"

Le due procedure pur rappresentando una descrizione dell'attività di gestione del sistema informativo effettuato dall'Area Sistemi Informatici, non fornisce quelle Istruzioni tecniche per la corretta gestione degli strumenti elettronici e dei dati trattati con il loro ausilio come richiamato dal Legislatore nella normativa in materia di privacy e di sicurezza dei sistemi informativi. Tali procedure, nell'ambito del sistema di gestione integrato, sono in via di revisione ed aggiornamento per colmare i limiti sopra descritti.

È stato adottato un regolamento aziendale (anche in ottemperanza alle Linee guida emanate dall'Autorità garante per la protezione dei dati personali sulla disciplina della navigazione in internet e sulla gestione della posta elettronica nei luoghi di lavoro) che dettaglia le modalità di accesso ed utilizzo degli strumenti informatici, di internet, della posta elettronica nell'ambito dello svolgimento delle proprie mansioni e compiti, ai fini di un corretto utilizzo degli strumenti stessi da parte degli amministratori, dipendenti e collaboratori dell'AMAP S.p.A., comprensivi dei controlli effettuati e delle eventuali sanzioni rispetto a violazioni del Regolamento.

Il Regolamento considera e definisce le regole interne di gestione degli specifici obblighi previsti dal Regolamento Privacy (Regolamento UE n. 679 del 2016) e dall'art. 29, 1°comma del D.Lgs. n. 242/1996 (in tema di controlli operati mediante il sistema informatico aziendale), nonché gli obblighi previsti dal disciplinare tecnico sulle misure minime di sicurezza allegato allo stesso Codice.

Il regolamento, inoltre, detta una disciplina per l'utilizzo degli strumenti informatici/telefonici aziendali e costituisce un utile strumento per sensibilizzare il personale su altri aspetti altrettanto importanti nella gestione dei sistemi informatici aziendali, quali il rispetto della normativa sulla tutela legale del software (e quindi il controllo sulla regolarità del software

presente nello stesso sistema informatico), e quella sulla tutela del know-how aziendale, quando queste importanti informazioni di proprietà dell'impresa sono custodite nel sistema informatico.

Indubbiamente l'adozione del Regolamento è stato un efficace strumento per limitare il rischio di insorgenza della responsabilità amministrativa a carico della società, prevista per i reati presupposto della presente procedura.

6.3.1 PROTOCOLLI SPECIFICI DI PREVENZIONE

Di seguito sono riportati i protocolli specifici di prevenzione nell'ambito di ciascuna area sensibile a rischio reato identificata e valutata attraverso l'analisi dei rischi allegata al modello organizzativo effettuato dalla AMAP S.p.A.

a. Installazione di apparecchiature per il danneggiamento dei dati contenuti nel sistema informativo aziendale.

Gli strumenti elettronici sono affidati ad ogni dipendente all'interno di AMAP S.p.a.

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare i reati presupposto esplicitamente richiamati dalla presente procedura.

Nella gestione del PC ci si atterrà agli specifici protocolli operativi previsti nel Regolamento di Utilizzo degli Strumenti Informatici adottati.

Come già detto in precedenza, per evitare l'utilizzo di postazioni informatiche e di accessi alla rete non autorizzati bisogna proceduralizzare una gestione delle Password come da Regolamento per l'Utilizzo dei Sistemi Informatici. In modo particolare bisogna verificare che le regole di gestione delle Password rispetti i criteri di sicurezza definiti dall'Organizzazione nell'ambito della sicurezza dei dati e di gestione della privacy secondo il Regolamento UE n. 679 del 2016.

b. Danneggiamento volontario di sistemi informatici o telematici.

Le regola e i protocolli indicati in precedenza per l'attività a) sono riportabili in modo identico anche per la prevenzione di eventuali danneggiamenti del sistema informatico e telematico.

In aggiunta a quanto indicato in precedenza è stata adottata un'Istruzione Operativa di "Incident e ripristino dati" inserita nel citato Regolamento che indichi le modalità operative da

utilizzare per evitare che il danneggiamento di una postazione o della rete abbia effetti irreversibili e possa essere ripristinata la regolare operatività.

6.4. CONTROLLO OPERATIVO

Il controllo operativo degli aspetti relativi ai reati cosiddetti "informatici" sono controllati secondo il sistema previsto dalla Procedura Operativa P.O. 9.p in revisione così come dal "Regolamento degli Strumenti Informatici".

Come già detto in precedenza sono esplicitati nella procedura e nell'apposito Regolamento le funzioni di controllo, di sorveglianza rispetto alle attività vietate e le modalità di intervento sul Sistema informativo aziendale di AMAP S.p.A.

7 FLUSSO INFORMATIVO ALL'ORGANISMO DI VIGILANZA

RESPONSABILE	Riferimento D.l.gs 231/2001	Riferimento normativo	FLUSSO ODV		PERIODICITA'	Mese di invio del flusso
COMM	ART. 24-bis D.Lgs. 231/2001 e art. 25-novies D.Lgs. 231/2001	Art. 635 bis e quater del codice penale e Art. 171 comma 1A-bis	Anomalie	back up dei dati	All'accadere dell'evento, annuali anche in assenza di eventi con una Relazione dell'Amministratore di Sistema	Entro il 31 Gennaio
				sistema di sicurezza logica e fisica del sistema informativo;		
				gestione degli strumenti informatici;		
				danneggiamento o rimozione di software in service per la gestione delle attività;		
				danneggiamento o rimozione di hardware in service per la gestione delle attività;		
				uso della rete locale e remota.		
COMM	ART. 24-bis D.Lgs. 231/2001 e art. 25-novies D.Lgs. 231/2001	Art. 635 bis e quater del codice penale e Art. 171 comma 1A-bis	Relazione annuale dell'Amministratore di sistema su eventuali incidenti durante la procedura di incident response e ripristino o attacchi da parte di virus o altre minacce al sistema informatico o installalzione di software non autorizzati o non licenziati		Annuale	Entro il 31 Gennaio