CONFINDUSTRIA

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D.LGS. N. 231/2001

PARTE SPECIALE C – REATI INFORMATICI

Roma, Giugno 2019

PARTE SPECIALE C

REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

INDICE

1. LE FATTISPECIE DI REATO 4
1.1. Premessa 4
1.2. I reati di cui all'art. 24-*bis* del Decreto Legislativo n. 231/2001 4

2. FUNZIONE DELLA PARTE SPECIALE C 5

3. PROCESSI SENSIBILI NELL'AMBITO DEI REATI INFORMATICI, TRATTAMENTO ILLECITO DEI DATI 6

4. PRINCIPI GENERALI DI COMPORTAMENTO 7

5. PRINCIPI DI CONTROLLO 9

6. FLUSSI INFORMATIVI 11

7. I CONTROLLI DELL'ORGANISMO DI VIGILANZA 11

1. LE FATTISPECIE DI REATO

1.1. Premessa

La presente Parte Speciale C è dedicata alla trattazione delle attività di gestione ed utilizzo dei sistemi informativi dell'Associazione 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.

Successivamente, si riporta il dettaglio delle fattispecie di reato la cui commissione potenziale è emersa durante l'analisi di Confindustria.

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 (art. 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.).

Per una trattazione completa delle ipotesi di reato previste dal D.Lgs. 231/2001, comprensiva del testo e di una casistica sintetica, si rimanda all'allegato "Elenco reati 231".

2. FUNZIONE DELLA PARTE SPECIALE C

Obiettivo della presente Parte Speciale C è far sì che i tutti i soggetti 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'Associazione, 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:

i) Modello organizzativo e di controllo;

ii) Codice di Comportamento;

iii) Sistema Disciplinare.

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

i) 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 organizzativo, 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 dell'Associazione e dalle stesse all'Organismo di Vigilanza, l'adozione di un sistema di *reporting* dell'Organismo di Vigilanza verso gli organi di Confindustria, la predisposizione di validi strumenti di controllo;

ii) L'adozione di un Codice di Comportamento che costituisce la carta dei valori della Confederazione, debitamente diffuso a tutti i componenti della struttura dell'Associazione, costantemente aggiornato e monitorato;

iii) L'adozione di un sistema disciplinare volto a garantire efficacia ed effettività alle prescrizioni interne.

In questa Parte Speciale sono 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 dell'Associazione definiti "sensibili" ovvero a rischio di specifico reato;

- i principi fondamentali di riferimento in attuazione dei quali dovranno essere adottate le procedure dell'Associazione 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 dell'Associazione 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

Le fattispecie di reato indicate *sub* par. 1 si applicano, in via potenziale, a tutte le Aree / Uffici / Servizi di Confindustria (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 dell'Associazione al fine di prevenire la commissione delle fattispecie di reato realizzabili previste dai sopraccitati articoli del Decreto.

I rischi potenziali di commissione di reati in questo ambito sono ascrivibili a tutte le aree e processi di Confindustria.

In particolare, le aree di attività ritenute più specificamente a rischio, individuate in sede di *risk assessment*, sono le seguenti:

- Gestione dei rapporti con soggetti pubblici (INPS, INAIL, Ag.Entrate, Centri Impiego, ecc.) per gli aspetti che riguardano adempimenti fiscali e/o la sicurezza e l'igiene sul lavoro e/o lo smaltimento dei rifiuti e/o i trattamenti previdenziali, nonché le relative verifiche ispettive che ne derivano;
- Gestione dei sistemi informativi.

Con riferimento alla suddetta Aree a Rischio, l'attività di Confindustria si ispira ai seguenti principi di controllo:

- chiara identificazione, mediante un sistema di deleghe e procure, dei soggetti deputati alla gestione del processo;
- esistenza di uno specifico protocollo che descrive ruoli, responsabilità, attività, modalità operative e controlli relativi alla gestione del processo;
- esistenza di separazione all'interno di ciascun processo, tra il soggetto che assume la decisione, il soggetto che la autorizza, il soggetto che la attua ed il soggetto cui è affidato il controllo del processo (c.d. segregazione delle funzioni);

- rispetto dei compiti, ruoli e responsabilità definiti dall'organigramma e dal sistema autorizzativo nella gestione del processo;
- archiviazione di tutta la documentazione connessa alla gestione del processo, anche al fine di garantirne la tracciabilità.

4. PRINCIPI GENERALI DI COMPORTAMENTO

Ai fini della presente Parte Speciale, sono stati individuati i Principi di Comportamento cui il personale di Confindustria, 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 dell'Associazione nel rispetto delle procedure definite;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi di Confindustria, evitando che terzi soggetti possano venirne a conoscenza e aggiornare periodicamente le password;
- 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 dell'Associazione alle sole attività lavorative.

Ciascun Responsabile di Area / 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 dedicato alla gestione dei sistemi informativi, in base al proprio ruolo ed alla propria responsabilità, **deve**:

- verificare la sicurezza della rete e dei sistemi informativi dell'Associazione 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" dell'Associazione a livello di sistemi informativi ed abilitazioni utente riconducibile ad una corretta segregazione dei compiti;
- garantire, sui diversi applicativi dell'Associazione, l'applicazione delle regole atte ad assicurare l'aggiornamento delle password dei singoli utenti;
- installare a tutti gli utenti esclusivamente software originali, debitamente autorizzati o 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 dell'Associazione, 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:

- produrre e trasmettere documenti in formato elettronico contenenti dati falsi e/o manipolati;
- intercettare fraudolentemente e/o diffondere comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti tecnologici (es. software) non autorizzati idonei ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- detenere, procurarsi, riprodurre e o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- 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;
- accedere ad aree riservate (quali server rooms, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente;
- 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;
- distruggere, deteriorare, cancellare, manipolare, eliminare informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad esso pertinenti o comunque di pubblica utilità;
- entrare nella rete dell'Associazione e nei programmi con un codice d'identificazione utente diverso da quello assegnato.

Inoltre, la funzione IT che svolge servizi di Information Technology ovvero Information Management devono ispirare la loro azione ai seguenti principi generali (anche con il supporto dell'outsourcer):

- Riservatezza - garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- Integrità - garanzia che ogni dato dell'Associazione sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- Disponibilità - garanzia di reperibilità di dati dell'Associazione in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Di seguito sono esposti i principi generali di controllo, volti alla prevenzione dei reati informatici e del trattamento illecito dei dati.

5. PRINCIPI DI CONTROLLO

In questa sezione si riportano i principi di controllo volti a prevenire i comportamenti illeciti previsti dall'art. 24-*bis* del D.Lgs. 231/2001.

Gestione dei rapporti con soggetti pubblici (INPS, INAIL, Ag.Entrate, Centri Impiego, ecc.) per gli aspetti che riguardano adempimenti fiscali e/o la sicurezza e l'igiene sul lavoro e/o lo smaltimento dei rifiuti e/o i trattamenti previdenziali, nonché le relative verifiche ispettive che ne derivano

- definizione di una modalità di raccolta, verifica e approvazione della documentazione da trasmettere alle controparti, con il supporto delle funzioni competenti.

Gestione dei Sistemi Informativi

- formale richiesta per la creazione/modifica/eliminazione delle utenze abilitate all'utilizzo dei sistemi informativi;
- previsione di costanti flussi informativi alla funzione IT in merito a nuove assunzioni, cambiamenti di ruolo o dimissioni del personale;
- definizione di criteri in merito alla corretta creazione e gestione delle password;
- definizione di password di accesso univoche;
- obbligo di rinnovo periodico della password;
- assegnazione, al personale dipendente, di un indirizzo di posta elettronica nominativo;
- revisione periodica delle utenze attive al fine di garantire la corretta profilazione e concessione dei privilegi a sistema;
- assegnazione dei profili di accesso degli utenti in base alle mansioni assegnate;
- formale autorizzazione per la connessione remota;
- previsione di un piano di backup periodico dei dati, file, programmi e sistemi operativi;
- verifica, con il supporto di fornitori esterni, del buon esito delle operazioni mediante controllo di appositi log;
- formale definizione di piani di continuità operativa o di disaster recovery;
- previsione di test di ripristino periodici;
- tracciabilità delle richieste di intervento di manutenzione sui sistemi informativi (evolutiva, correttiva e ordinaria);
- formale definizione di un processo di change management (inclusa la formale autorizzazione degli interventi di manutenzione);

- formale autorizzazione della messa in produzione di applicativi sviluppati da terze parti;
- registrazione degli accessi ai sistemi tramite file di log immodificabili;
- accesso ai file di log riservato al personale autorizzato;
- periodico monitoraggio dei log (di accesso e di attività) relativi alle utenze privilegiate inclusi gli Amministratori di sistema;
- utilizzo di firewall a protezione della rete interna;
- utilizzo di appositi programmi antivirus aggiornati automaticamente su server e client;
- previsione di filtri antispamming, antiphishing e antivirus per i server di posta elettronica;
- previsione di un flusso informativo nei confronti della funzione IT in caso di messaggi di posta elettronica sospetti;
- archiviazione dei messaggi di posta elettronica in entrata ed in uscita;
- formale individuazione dei soggetti incaricati alla configurazione degli apparati di rete;
- formale autorizzazione, da parte dei soggetti incaricati, delle variazioni sugli apparati di rete;
- verifiche periodiche sulla sicurezza di rete tramite attività di vulnerability scanning e health checking;
- previsione di reportistica periodica al fine di rilevare anomalie della rete e relativo monitoraggio;
- definizione di criteri di assegnazione delle risorse e servizi informatici;
- definizione di livelli autorizzativi per l'assegnazione delle risorse e servizi informatici;
- catalogazione delle risorse informatiche assegnate e verifica periodica delle stesse;
- previsione di attività di monitoraggio / controllo periodico dell'efficacia e operatività del sistema di gestione della sicurezza informatica;
- utilizzo di controlli crittografici per la protezione delle informazioni e regolamentazione della gestione delle chiavi crittografiche;
- previsione di regole formalizzate connesse alla gestione degli incidenti e dei problemi di sicurezza informatica.

6. FLUSSI INFORMATIVI

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.

Sarà compito dell'OdV definire e comunicare alle Unità Organizzative coinvolte nella gestione delle attività potenzialmente a rischio le modalità e le tempistiche di comunicazione dei flussi informativi relativi alle stesse.

Le modalità operative per la gestione delle attività in oggetto sono disciplinate anche all'interno del Codice di Comportamento.

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 e al trattamento illecito dei 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 interne in essere.

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

Di detti controlli l'Organismo di Vigilanza riferisce al Direttore Generale, nonché, annualmente, al Collegio dei Revisori.