"PARTE SPECIALE F"

ai sensi del D.lgs. n. 231/2001

"Prevenzione dei Reati Informatici e di Trattamento Illecito dei Dati, dei Reati in materia di Violazione del Diritto d'Autore"

Approvazione: *Consiglio di Amministrazione*

INDICE

1 Premessa

La presente Parte Speciale del Modello Organizzativo è dedicata alla trattazione dei "*Reati Informatici e di Trattamento Illecito dei Dati oltre che dei* R*eati in materia di Violazione del Diritto d'Autore*" così come individuati negli articoli artt. 24-bis e 25-novies del D.lgs. n. 231/2001 e rappresenta il sistema di protocolli adottati dalla Fondazione Cassa di Risparmio di Padova e Rovigo (di seguito anche "Fondazione" o "Ente") al fine di contrastare il rischio di commissione dei suddetti reati da parte dei Destinatari del Modello Organizzativo per quanto coinvolti nell'espletamento delle "attività sensibili".

La presente Parte Speciale è stata predisposta sulla base dell'Analisi dei Rischi (cfr. PV. n. 248 del 07/02/2014) e a successivi aggiornamenti (cfr. PV n. 317 del 11/04/2017) a cui si rimanda per le considerazioni di dettaglio.

1.1 Revisioni

N° Rev.	Data rev.	Note
1.0	01/12/2016	P.V. CA n. 309 - Prima emissione
2.0	13/04/2018	P.V. CA n.334 – modifiche conseguenti all'introduzione di nuovi reati nel D.lgs.n.231/2001, oltre al cambiamento della struttura e funzionamento organizzativo.

2 Descrizione fattispecie di reato

Tutte le condotte rilevanti ai fini della legge penale e delle leggi speciali applicabili sono rappresentate nell'allegato "*Elenco dei Reati*", parte integrante del Modello Organizzativo, adottato dall'Ente, cui si rimanda per la trattazione approfondita della materia.

Sulla base delle analisi condotte sui processi e sulle attività dell'Ente, i principi contenuti nella presente Parte Speciale sono volti a presidiare, principalmente, il rischio di commissione dei seguenti reati:

- Art. 491 bis c.p. - documenti informatici
- Art. 615-ter c.p. -accesso abusivo ad un sistema informatico
- Art. 615-quater - c.p. detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- Art. 615-quinquies c.p. - diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- Art. 617-quater c.p. - intercettazione, impedimento o interruzione illecita di comunicazioni informatiche e telematiche
- Art. 617-quinquies c.p. - diffusione di apparecchiature, dispositivi e programmi informatici diretti a danneggiare o interrompere un sistema informatico e telematico
- Art. 635-bis c.p. - danneggiamento di informazioni, dati e programmi informatici
- Art. 635-ter c.p. - danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico, o comunque di pubblica utilità
- Art. 635-quater c.p. - danneggiamento di sistemi informatici o telematici
- Art. 635-quinquies c.p. - danneggiamento di sistemi informatici o telematici di pubblica utilità.

Le analisi condotte sui processi e sulle attività svolte dall'Ente hanno portato a ritenere non applicabili alle Fondazioni i suddetti reati presupposto o comunque a valutare alquanto remoto il rischio di incorrere nella realizzazione del reato presupposto di frode informatica del certificatore di firma elettronica art. 640-quinquies c.p..

- Art. 171-ter L. n. 633/1941 - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio.

3 Attività Sensibili e Flussi informativi

L'analisi dei processi e delle aree operative della Fondazione ha consentito di individuare le principali attività caratteristiche (di seguito attività sensibili) potenzialmente esposte al compimento di uno dei reati oggetto della presente Parte Speciale e previsti dal D.lgs. n. 231/01. L'esito di tale analisi è di seguito riportato.

Le attività sensibili sono inerenti alla gestione delle infrastrutture tecnologiche, che attualmente è affidata alla società strumentale di cui l'Ente si avvale avendo sottoscritto un contratto di outsourcing con la stessa, del processo di gestione della comunicazione e del processo erogativo.

Ai fini dell'efficace vigilanza sull'attuazione del Modello Organizzativo i Destinatari, in ragione del proprio ruolo e delle proprie responsabilità, sono tenuti alla trasmissione dei principali flussi informativi verso l'Organismo di Vigilanza con la cadenza periodica prevista, salvo esigenze specifiche.

Tra i flussi informativi principali dei quali l'Organismo di Vigilanza deve essere periodicamente destinatario, rientrano, a mero titolo di esempio e senza pretesa di completezza, oltre a quanto già indicato nella "*Parte Generale*" del Modello, le principali informazioni, dati e notizie elencati all'interno del documento "*Flussi Informativi*".

In ogni caso all'Organismo di Vigilanza sono conferiti tutti i poteri per richiedere in ogni momento qualsiasi informazione, dato, documento, notizia ai Destinatari del Modello organizzativo.
I Destinatari del Modello organizzativo dovranno fornire senza indugio quanto richiesto all'Organismo di Vigilanza.

Resta altresì fermo il principio che ogni informazione o notizia che ai sensi del Modello organizzativo possa considerarsi rilevante dovrà essere trasmessa senza indugio all'Organismo di Vigilanza.

4 Protocolli Generali

Nell'espletamento delle attività a rischio è espressamente fatto obbligo ai Destinatari di collaborare e agire in accordo a i comportamenti generali, definiti all'interno del successivo paragrafo 4.1., i comportamenti specifici definiti all'interno del paragrafo 5 oltre che a trasmettere i flussi informativi all'Organismo di Vigilanza.
Per tutto quanto non espressamente disciplinato dalla presente Parte Speciale, i Destinatari sono tenuti a osservare i principi etici e di comportamento contenuti nel "Codice Etico e Comportamentale" e le "procedure" dell'Ente applicabili.

4.1 Comportamenti espressamente richiesti

Lo svolgimento delle attività è riservato alle funzioni e ai soggetti formalmente preposti e autorizzati, per i quali vige l'obbligo di rispettare e dare attuazione ai regolamenti e alle procedure formalizzate oltre che di raccogliere e conservare la documentazione utile ai fini probatori.

I responsabili delle funzioni che svolgono o partecipano ad una o più attività sensibili, devono fornire ai propri collaboratori adeguate direttive sulle modalità di condotta operativa da adottare, secondo le peculiarità del proprio ambito di attività, trasferendo la conoscenza della normativa esterna ed interna e la consapevolezza delle situazioni a rischio di reato.

4.2 Comportamenti espressamente vietati

In nessun caso il perseguimento dell'interesse o del vantaggio dell'Ente può giustificare una condotta non onesta o non rispettosa della legge.

5 Protocolli Specifici

PROCESSO di GESTIONE delle INFRASTRUTTURE

attività caratteristiche valutate come "attività sensibili" alla commissione dei reati:

– Architettura infrastruttura tecnologica

-Assegnazione Dotazioni

– Gestione Reti e Collegamenti

– Gestione Abilitazioni e Autenticazioni

- Progettazione, Sviluppo, Test, Collaudo e Rilascio del Software

- Disaster Recovery (back up on site e off site, snapshosts)

fattispecie esemplificativa di inadempimento che potrebbe dare luogo alla commissione dei reati:

- *installazione di software contraffatto;*
- *duplicazione abusiva di un programma coperto da licenza;*
- *installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti fra più sistemi (es. spyware);*
- *utilizzo di supporti removibili o di altre apparecchiature per l'esecuzione di attività improprie;*
- *riproduzione, diffusione, comunicazione o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza;*
- *danneggiamento, distruzione e cancellazione atte ad alterare o sopprimere dati, informazioni programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità;*
- *danneggiamento, in tutto o in parte, di sistemi informatici o telematici altrui o impedimento del funzionamento;*
- *accesso abusivo, ossia eludendo una qualsiasi forma, anche minima, di barriere all'accesso, in un sistema informatico o telematico protetto da misure di sicurezza;*
- *intercettazione, impedimento o interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.*

Entità organizzative prevalentemente coinvolte*:*

Segretario Generale, Area Amministrazione e Controllo di gestione, Area Segreteria e Affari legali, Auxilia Spa (Area Infrastrutture e Sistemi Informativi) e tutte le altre aree coinvolte nella gestione delle infrastrutture tecnologiche.

PROCESSO di GESTIONE delle INFRASTRUTTURE	
Protocolli	***Descrizione***
Codice Etico e Comportamentale	*Art. 23 Personale e collaboratori, Art. 28 Informazioni, Art. 29 Infrastrutture*
Comportamenti Richiesti	*È fatto obbligo di individuare il Responsabile della privacy e l'Amministratore di sistema conferendo deleghe e poteri risultanti da atto scritto.* *È fatto obbligo di installare software ed usare programmi software rilasciati, testati e autorizzati.* *È fatto obbligo di accedere ai sistemi informativi e database di proprietà di terzi solo ed esclusivamente ai soggetti formalmente preposti e autorizzati.* *È fatto obbligo di riservare l'implementazione di software (progettazione, sviluppo e rilascio) alle funzioni e ai soggetti formalmente preposti e autorizzati.* *È fatto obbligo di garantire il corretto e periodico salvataggio dei dati.* *È fatto obbligo di garantire che ogni dato e informazione sia realmente quello originariamente immesso nel sistema informatico e sia modificato esclusivamente in modo legittimo e tracciabile.* *È fatto obbligo di segnalare eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche.* *È fatto obbligo di dotarsi di strumenti che consentano di filtrare l'accesso e/o ricezione di materiale informatico.*
Comportamenti Vietati	*È fatto divieto di fornire informazioni non appropriate, compromettendo l'affidabilità delle stesse informazioni a qualsiasi scopo.* *È fatto divieto di aggirare o tentare di aggirare le misure di sicurezza (Antivirus, Firewall, proxy server, ecc.).* *È vietato danneggiare informazioni, dati e programmi informatici o telematici altrui.* *Non è consentito l'utilizzo in maniera illecita o impropria dei codici di accesso delle infrastrutture e degli applicativi, anche di proprietà di terzi.* *Non è consentito l'accesso senza autorizzazioni e privilegi al fine di consultare e gestire dati e informazioni contenute negli archivi dell'Ente e di terzi; è altresì vietato manipolare i dati protetti da misure di sicurezza di database dell'Ente e di proprietà di terzi.* *Non è concesso l'utilizzo in maniera illecita o impropria dei codici di accesso delle infrastrutture e degli applicativi, anche di proprietà terzi.* *È fatto divieto di accedere ai database di proprietà di terzi al fine di modificare, cancellare dati, file o programmi, danneggiare o alterare l'integrità, ovvero l'accuratezza e la completezza delle informazioni e la loro validità.* *È fatto divieto di detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate.* *È fatto divieto di copiare dati su supporti removibili salvo per esigenze operative temporanee e comunque tali memorizzazioni devono essere cancellate al termine delle operazioni*
Regolamenti, Procedure e processi	*Documento Programmatico per la Sicurezza, Codice Informatico (ex Disciplinare Tecnico)* *Procedura Gestione Sistemi Informativi*
Flussi Informativi	*Flussi Informativi (Documento di supporto)*

PROCESSO di GESTIONE DELLA COMUNICAZIONE e MEDIA

attività caratteristiche valutate come "attività sensibili" alla commissione dei reati:

- Sito Web e Social media

fattispecie esemplificativa di inadempimento che potrebbe dare luogo alla commissione dei reati:

- *immissione nella rete internet (es.: sito ufficiale, Museo on Line) di un'opera altrui protetta dal diritto d'autore, rendendola liberamente scaricabile da chiunque o attribuendosene la paternità.*

Entità organizzative prevalentemente coinvolte*:*

Consiglio di Amministrazione, Presidente, Segretario Generale, Area Comunicazione, Auxilia Spa (Area Infrastrutturee Sistemi Informativi) e tutte le altre funzioni che a vario titolo concorrono alle attività di comunicazione.

PROCESSO di GESTIONE DELLA COMUNICAZIONE e RELAZIONI ESTERNE	
Protocolli	***Descrizione***
Codice Etico e Comportamentale	*Art. 20 Tutela del Patrimonio artistico, Art. 23 Personale e collaboratori, Art. 28 Informazioni, Art. 29 Infrastrutture*
Comportamenti Richiesti	*È fatto obbligo che il caricamento dei contenuti sul sito internet sia effettuato e gestito solo da parte dei soggetti chiaramente identificati.* *È fatto obbligo che i contenuti caricati siano predisposti, controllati e autorizzati da soggetti distinti garantendo la separatezza organizzativa.* *È fatto obbligo di osservare tutte le misure di sicurezza, fisiche e logiche applicate dall'Ente.* *È fatto obbligo di prevedere a livello di contratto la presenza di regole inerenti il rispetto delle norme in materia di violazione del diritto d'autore.*
Comportamenti Vietati	*È fatto divieto di riprodurre o copiare e diffondere anche attraverso internet o i social network opere protette dal diritto di autore.* *È fatto divieto di comunicare informazioni riservate, a prescindere da come queste vengono poi utilizzate dal confidente.* *È fatto divieto di utilizzare e diffondere informazioni riservate in modo inappropriato e abusivo.* *È fatto divieto di diffondere le opere soggette al diritto d'autore in qualsiasi forma senza l'autorizzazione del titolare o in violazione del divieto imposto dal costitutore.*
Regolamenti, Procedure e processi	*Procedura Relazioni con i Media* *Documento Programmatico per la Sicurezza e Codice Informatico (ex Disciplinare Tecnico)*
Flussi Informativi	*Flussi Informativi (Documento di supporto)*

PROCESSO di GESTIONE delle EROGAZIONI

attività caratteristiche valutate come "attività sensibili" alla commissione dei reati:

– Realizzazione Progetti di Fondazione (es. mostre, progetti nel settore della ricerca scientifica)

fattispecie esemplificativa di inadempimento che potrebbe dare luogo alla commissione dei reati:

- *utilizzo abusivo dell'opera dell'ingegno altrui (riproduzione, trascrizione, diffusione in qualsiasi forma, rappresentazione o esecuzione in pubblico)*

Entità organizzative prevalentemente coinvolte*:*

Consiglio di Amministrazione, Presidente, Segretario Generale, Area Attività Istituzionale, Area Pianificazione e Valutazione, Area Comunicazione, e tutte le altre aree coinvolte nella gestione delle erogazioni.

PROCESSO di GESTIONE delle EROGAZIONI	
Protocolli	***Descrizione***
Codice Etico e Comportamentale	*Art. 7 Obbligo di Correttezza, Art. 9 Trasparenza dell'Attività e delle Informazioni, Art. 18 Tracciabilità delle Attività Economiche, Art. 20 Tutela del Patrimonio artistico, Art. 28 Informazioni*
Comportamenti richiesti	*È fatto obbligo di acquisire il consenso all'utilizzo di opere dell'ingegno altrui da parte del soggetto titolato alla prestazione dello stesso.* *È fatto obbligo di regolamentare tali aspetti nel rapporto contrattuale.*
Comportamenti Vietati	*È fatto divieto di sfruttare senza avere titolo le opere dell'ingegno altrui.*
Regolamenti, Procedure e processi	*Procedura Bandi e Richieste di Terzi* *Procedura Progetti di Fondazione*
Flussi Informativi	*Flussi Informativi (Documento di supporto)*