PARTE SPECIALE "B"

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

Entrata in vigore: Delibera CdA n° D_64_17 del 13.10.2017

INDICE

B.1 DESTINATARI DELLA PARTE SPECIALE E PRINCIPI GENARALI DI COMPORTAMENTO

La presente Parte Speciale del Modello è finalizzata alla trattazione dei delitti informatici e di trattamento illecito dei dati e fa riferimento a comportamenti che possano essere posti in essere dai Destinatari del Modello operanti nelle aree a rischio reato (cfr. paragrafo B.2 della presente Parte Speciale).

La presente Parte Speciale, oltre agli specifici principi di comportamento relativi alle aree a rischio reato, richiama quanto previsto nel Codice Etico del Fondo alla cui osservanza sono tenuti tutti i Destinatari e prevede l'espresso divieto a carico dei Destinatari di porre in essere comportamenti:

- tali da integrare le fattispecie di reato previste dall'art. 24 bis del D.Lgs. 231/01 (per maggiori dettagli si veda l'Allegato 3 del Modello "*Elenco dei reati presupposto"*), anche nella forma del concorso o del tentativo, ovvero tali da agevolarne la commissione;
- non conformi alle leggi, ai regolamenti vigenti, nonché alle procedure del Fondo o, comunque, non in linea con i principi espressi nel Modello e nel Codice Etico.

Inoltre, per tutti coloro che operano per conto del Fondo, nelle attività relative all'utilizzo ed alla gestione di sistemi, strumenti, documenti o dati informatici, è fatto divieto in particolare di:

- utilizzare gli strumenti, i dati ed i sistemi informatici e telematici in modo da recare danno a terzi, in particolare interrompendo il funzionamento di un sistema informatico o alterando dati o programmi informatici, anche a seguito dell'accesso abusivo, ovvero dell'intercettazione di comunicazioni;
- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- detenere o diffondere indebitamente codici, programmi, parole chiave o altri mezzi atti all'accesso ad un sistema informatico o telematico di soggetti pubblici o privati, al fine di acquisire informazioni riservate;
- detenere o diffondere indebitamente codici, programmi, parole chiave o altri mezzi atti al danneggiamento informatico;
- alterare o falsificare documenti informatici di qualsiasi natura o utilizzare indebitamente la firma elettronica;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o *software* allo scopo di danneggiare un sistema informatico o telematico di soggetti pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- porre in essere comportamenti in contrasto con leggi e regolamenti in materia di protezione e sicurezza di dati personali e sistemi informatici (in particolare, Codice in materia di protezione dei dati personali; provvedimenti del Garante della Privacy, ecc.).

Pertanto, i Destinatari sono tenuti a:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi connessi all'espletamento delle mansioni;
- evitare di introdurre e/o conservare, a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo se acquisiti con il loro espresso consenso e per motivi strettamente lavorativi;
- evitare di trasferire all'esterno e/o trasmettere *files*, documenti o qualsiasi altra documentazione riservata di proprietà del Fondo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
- evitare l'utilizzo di strumenti *software* e/o *hardware* atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- utilizzare la connessione ad internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività lavorative;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle strutture competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature del Fondo solo prodotti ufficialmente acquistati dallo stesso;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di *software*;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni del Fondo;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza del Fondo per la protezione ed il controllo dei sistemi informatici.

Ai fini dell'attuazione dei comportamenti di cui sopra:

- sono predisposti strumenti tecnologici atti a prevenire e/o impedire la realizzazione di illeciti informatici da parte degli esponenti del Fondo attraverso, in particolare, l'uso indebito o non autorizzato delle *password*, la detenzione o installazione di *software* non previsto dalle procedure del Fondo, ivi compresi *virus* e s*pyware* di ogni genere e natura e dispositivi atti all'interruzione di servizi o alle intercettazioni, il collegamento non consentito di *hardware* alla rete del Fondo. Tali misure in particolare prevedono regole in merito:
  - alle restrizioni all'accesso fisico ai luoghi in cui sono collocati gli strumenti informatici/telematici;
  - all'attribuzione e revoca delle *password*, tenendo conto delle mansioni per la quale viene richiesta / concessa;
  - alla rimozione dei diritti di accesso al termine del rapporto di lavoro;
  - al controllo e alla tracciabilità degli accessi;
  - alle modalità di svolgimento delle attività di gestione e manutenzione dei sistemi;
  - alla previsione di controlli sulla idoneità della rete del Fondo e sul suo corretto instradamento;
- sono adottate specifiche misure di protezione volte a garantire l'integrità delle informazioni messe a disposizione del pubblico tramite la rete internet;
- sono adottati specifici strumenti per l'individuazione, prevenzione e ripristino dei sistemi rispetto a *virus* ed altre vulnerabilità;
- sono definiti ed implementati controlli specifici per la protezione dei documenti sulla base della loro classificazione, attraverso: la crittografia dei documenti; la restrizione degli accessi in lettura/scrittura sulla base delle liste di distribuzione definite; la corretta conservazione dei file;
- i fabbisogni di materiale IT sono dettagliati nel budget preventivo del Fondo;
- sono previsti e attuati programmi di informazione, formazione e sensibilizzazione rivolti al personale del Fondo al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche in dotazione al Fondo.

B.2 AREE POTENZIALMENTE A RISCHIO E PRINCIPI DI CONTROLLO PREVENTIVO

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

I reati di cui all'art. 24 bis del Decreto hanno come presupposto l'impiego di sistemi, strumenti e programmi informatici. In tale contesto, è opportuno segnalare che gran parte dei Destinatari del Fondo utilizzano ordinariamente strumenti di tipo informatico ed hanno, di conseguenza, una astratta possibilità di accesso a strumenti e dati informatici e telematici nel contesto dell'ordinaria attività lavorativa. Pertanto, con riferimento ai delitti informatici ed al trattamento illecito dei dati contemplati dall'art. 24 bis del Decreto, in considerazione della diffusione presso il Fondo di sistemi e strumenti informatici, essi potrebbero essere astrattamente posti in essere in ogni ambito di attività e, conseguentemente, il loro rischio di commissione è stato valutato come **diffuso** e non localizzato a specifiche aree o strutture del Fondo.

L'analisi dei processi del Fondo ha consentito di individuare nell'Area ICT la struttura a presidio del rischio di astratta realizzazione delle fattispecie di reato in oggetto. Tale Area si occupa, per quanto di propria competenza, delle attività di gestione, manutenzione e monitoraggio dei sistemi informatici, dal processo di autenticazione e gestione dei profili utente alla protezione delle reti, della postazione di lavoro e degli accessi da e verso l'esterno, nonché della sicurezza fisica e logica dell'architettura informatica e della gestione dei documenti elettronici e degli output di sistema e dei dispositivi di memorizzazione.

Pertanto, ciò premesso, in base all'analisi dei processi del Fondo mappati ai fini del *risk assessment*, sono state individuate le aree a rischio reato sotto indicate. Per ognuna di queste, così come indicato nella Parte Generale del Modello (cfr. paragrafo 2.4.3), sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati previsti dal Decreto ed indicati nell'Allegato 3 del Modello. Sono stati inoltre enucleati, in via esemplificativa e non esaustiva, i principali controlli preventivi previsti con riferimento alle attività che sono poste in essere nelle aree a rischio reato.

Area a rischio n. 1

GESTIONE E MANUTENZIONE DEGLI APPLICATIVI E DEI SISTEMI INFORMATICI

- RUOLI E FUNZIONI COINVOLTE

  Direzione, Area ICT

- ATTIVITÀ SENSIBILI

  a) Gestione dello sviluppo e della manutenzione dei *software*;

  b) Gestione della sicurezza logica;

  c) Gestione della sicurezza fisica;

  d) Gestione dei *backup*.

  e) Gestione dei fornitori in ambito IT.

- REATI ASTRATTAMENTE IPOTIZZABILI ED ESEMPLIFICATIVE MODALITÀ DI COMMISSIONE

  a) Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)

  A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso l'accesso al sistema informatico di *competitors* o di altri soggetti, mediante l'utilizzo di sistemi informatici aziendali ovvero mediante l'utilizzo di *username* e *password* personali ottenute in maniera fraudolenta e/o per mezzo di tecniche di *hacking* o per appropriazione indebita da parte di utenti/specialisti IT. Il vantaggio può configurarsi, ad esempio, nell'acquisire dati ed informazioni riservate di concorrenti o di altri soggetti, nel manipolare / alterare dati prima o durante il loro inserimento nella memoria del sistema informatico, nell'inserire abusivamente istruzioni in un programma in modo che il sistema informatico operi in modo diverso da quello predeterminato dal legittimo titolare e, in questo modo, procurare vantaggi al Fondo; nell'inserire abusivamente un programma nel sistema informatico per causarne l'arresto attraverso delle istruzioni del tutto incoerenti o contrastanti rispetto a quelle predisposte per il funzionamento del sistema informatico medesimo e, in tal modo, procurare vantaggi al Fondo; nel distruggere, sui sistemi dei concorrenti o di altri soggetti, le informazioni e la documentazione relativa a loro prodotti/progetti e ottenere un vantaggio competitivo;

  b) Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)

  A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso:

  - la violazione fisica o logica delle protezioni ai sistemi delle infrastrutture tecnologiche dei concorrenti o di altri soggetti al fine di ottenere, direttamente o indirettamente, un vantaggio economico e/o finanziario e/o impedirne l'attività o danneggiare in altro modo i concorrenti;

- l'alterazione o l'accesso indebito a dati e/o programmi in ambiente di produzione, al fine di produrre dati ed informazioni di bilancio false e conseguire, in genere, un vantaggio economico, patrimoniale e/o finanziario per il Fondo;
- il danneggiamento di informazioni, dati o programmi informatici commesso dal personale incaricato della loro gestione, nello svolgimento delle attività di manutenzione e aggiornamento di propria competenza, al fine di distruggere dati ed informazioni compromettenti che, se diffusi, arrecherebbero un danno al Fondo;

c) Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso:

- l'acquisizione indebita di credenziali di accesso ai sistemi ed utilizzazione non autorizzata di un elaboratore o di un sistema o di una rete informatica senza diritto al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione;
- il danneggiamento di informazioni, dati e programmi informatici utilizzati da Enti Pubblici al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione;

d) Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 bis c.p.)

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso l'acquisizione indebita di credenziali di accesso ai sistemi e danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso Enti Pubblici (INPS, INAIL, ISTAT, Uffici Giudiziari, Polizia, ecc.), in quanto prova della colpevolezza del Fondo nel corso di un procedimento o di un'indagine giudiziaria.

Area a rischio n. 2

AMMINISTRAZIONE DEL PERSONALE

- RUOLI E FUNZIONI COINVOLTE

  Direzione, Area Amministrazione

- ATTIVITÀ SENSIBILI

a) Installazione, manutenzione, aggiornamento e gestione di *software* di soggetti pubblici utilizzati anche per lo scambio di dati ed informazioni riguardanti tutti gli adempimenti previdenziali ed assistenziali.

- REATI ASTRATTAMENTE IPOTIZZABILI ED ESEMPLIFICATIVE MODALITÀ DI COMMISSIONE

a) Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso:

- l'acquisizione indebita di credenziali di accesso ai sistemi ed utilizzazione non autorizzata di un elaboratore o di un sistema o di una rete informatica senza diritto al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione;
- l'acquisizione indebita di credenziali di accesso ai sistemi e danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso Enti Pubblici (INPS, INAIL, ISTAT, Uffici Giudiziari, Polizia, ecc.), in quanto prova della colpevolezza del Fondo nel corso di un procedimento o di un'indagine giudiziaria;
- il danneggiamento di informazioni, dati e programmi informatici utilizzati da Enti Pubblici al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione.

Area a rischio n. 3

GESTIONE DEI RAPPORTI CON L'AMMINISTRAZIONE FINANZIARIA

- RUOLI E FUNZIONI COINVOLTE

Direzione, Area Amministrazione, Affari Legali e Gare

- ATTIVITÀ SENSIBILI

a) Installazione, manutenzione, aggiornamento e gestione di *software* di soggetti pubblici utilizzati anche per lo scambio di dati ed informazioni riguardanti tutti gli adempimenti fiscali.

- REATI ASTRATTAMENTE IPOTIZZABILI ED ESEMPLIFICATIVE MODALITÀ DI COMMISSIONE

a) Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)

A mero titolo esemplificativo e non esaustivo, il reato si potrebbe configurare attraverso:

- l'acquisizione indebita di credenziali di accesso ai sistemi ed utilizzazione non autorizzata di un elaboratore o di un sistema o di una rete informatica senza diritto al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione;

- l'acquisizione indebita di credenziali di accesso ai sistemi e danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso Enti Pubblici (INPS, INAIL, ISTAT, Uffici Giudiziari, Polizia, Agenzia delle Entrate, ecc.), in quanto prova della colpevolezza del Fondo nel corso di un procedimento o di un'indagine giudiziaria;
- il danneggiamento di informazioni, dati e programmi informatici utilizzati da Enti Pubblici al fine di falsificare, modificare o alterare informazioni riguardanti il Fondo presso i sistemi informatici della Pubblica Amministrazione.

➢ PRINCIPI DI CONTROLLO PREVENTIVO RELATIVI ALLE AREE A RISCHIO N. 1, 2 e 3

Oltre ai principi di controllo preventivo descritti con riferimento alle aree a rischio di cui alla Parte Speciale "A" del presente Modello, le attività del Fondo - a mitigazione dei fattori di rischio correlati ai reati informatici di cui all'art. 24 bis del Decreto e con riferimento alle aree in oggetto - si ispirano ai seguenti principali principi di controllo preventivo:

- rispetto dei ruoli, compiti e responsabilità definiti dall'organigramma del Fondo e dal sistema autorizzativo nella gestione di sistemi, strumenti, documenti o dati informatici;
- formale identificazione dei soggetti deputati alla gestione di sistemi, strumenti, documenti o dati informatici;
- corretto e sicuro funzionamento degli elaboratori di informazioni;
- definizione delle modalità di registrazione e deregistrazione per accordare e revocare, in caso di cessazione o cambiamento del tipo di rapporto o dei compiti assegnati, l'accesso a tutti i sistemi e servizi informativi, anche di terzi;
- rivisitazione periodica dei diritti d'accesso degli utenti;
- accesso ai servizi di rete esclusivamente da parte degli utenti specificamente autorizzati;
- controlli formalizzati sugli accessi atti a presidiare il rischio di accesso non autorizzato alle informazioni, ai sistemi, alle reti e alle applicazioni, nonché atti a prevenire danni ed interferenze ai locali ed ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature;
- segregazione delle funzioni al fine di garantire operativamente la separazione del livello esecutivo da quello approvativo;
- segmentazione della rete al fine di assicurare che le connessioni ed i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni utilizzate dal Fondo;
- autenticazione individuale degli utenti tramite codice identificativo dell'utente e *password* o tramite altro sistema idoneo a garantire un adeguato livello di sicurezza;
- formale autorizzazione, nel rispetto delle deleghe in essere, all'accesso alle informazioni;
- controlli di sicurezza dedicati a garantire l'integrità, disponibilità e riservatezza delle informazioni sensibili;

- utilizzo di dispositivi *hardware* e *software* dedicati per l'implementazione delle politiche di navigazione in internet e scambio delle informazioni (*firewall*, *proxy server*, ecc.);
- meccanismi di protezione per lo scambio di informazioni tramite internet, posta elettronica e dispositivi rimovibili;
- implementazione di misure di sicurezza atte a garantire l'accesso alle informazioni da parte di terze parti solo previa autorizzazione formale e nel rispetto degli accordi di riservatezza e confidenzialità stipulati;
- implementazione di ambienti logicamente e fisicamente separati al fine di controllare e testare le modifiche software fino al rilascio in produzione;
- definizione formale delle modalità di protezione da *software* pericolosi;
- definizione formale delle modalità di gestione dei *back-up* delle informazioni e dei *software*;
- formale classificazione delle informazioni e dei sistemi informatici gestiti dal Fondo;
- controlli formalizzati atti a presidiare il rischio di appropriazione e modifica indebita delle informazioni di proprietà del Fondo con conseguente perdita di autenticità, riservatezza ed integrità dell'*asset* informativo;
- definizione delle modalità di custodia dei dispositivi di memorizzazione (ad es. chiavi USB, CD, *hard disk* esterni, ecc.) e previsione di regole di *clear screen* per gli elaboratori utilizzati;
- definizione delle tempistiche per la chiusura delle sessioni inattive;
- formale definizione dei processi di *change management* con indicazione dei ruoli coinvolti nell'iter autorizzativo e della segregazione dei compiti garantita nella gestione dei cambiamenti;
- formale definizione delle modalità operative per l'individuazione e la gestione degli incidenti e dei problemi;
- verifica periodica di tutti gli incidenti singoli e ricorrenti al fine di individuarne le relative cause;
- verifica periodica dei *trend* sugli incidenti e sui problemi al fine di individuare le azioni preventive al verificarsi di problemi in futuro;
- valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi e che tenga conto della normativa applicabile in materia e dei principi etici del Fondo;
- formale definizione dei rapporti con gli *outsourcer* in materia informatica, redatti attraverso specifici contratti approvati nel rispetto delle deleghe e procure in essere;
- previsione di specifiche attività di formazione ed aggiornamenti periodici sulle procedure di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;

- obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa per i dipendenti e per i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
- tracciabilità di tutte le operazioni effettuate per la gestione dei sistemi, strumenti, documenti o dati informatici utilizzati dal Fondo.

B.3 COMPITI DELL'ORGANISMO DI VIGILANZA E FLUSSI INFORMATIVI

L'OdV vigila sul funzionamento e sull'osservanza del Modello e ne cura l'aggiornamento, al fine di assicurarne l'idoneità e l'efficacia a prevenire i reati di cui alla presente Parte Speciale.

In tal contesto, devono intendersi qui integralmente richiamati i compiti attribuiti all'Organismo ed i flussi informativi verso lo stesso già dettagliati nella Parte Generale del Modello.