Modello di organizzazione, gestione e controllo

(*D. Lgs. n. 231/2001)*

Parte Speciale 2

Delitti informatici e trattamento illecito di dati (articolo 24-bis)
Delitti in materia di diritto d'autore (articolo 25-novies)

Destinatari e finalità della Parte Speciale – Delitti informatici e trattamento illecito dei dati

Sono destinatari (di seguito i "Destinatari") della presente Parte Speciale del Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001 della Villaservice S.p.a. (di seguito la "Società") e si impegnano al rispetto del contenuto dello stesso:

- il Presidente (soggetto *apicale*);
- il Consiglio di amministrazione (soggetto *apicale*);
- il Direttore tecnico e i dipendenti della Società (cosiddetti soggetti interni *sottoposti ad altrui direzione*).

Limitatamente allo svolgimento delle attività a rischio a cui essi eventualmente partecipano, possono essere destinatari di specifici obblighi, strumentali ad un'adeguata esecuzione delle attività di controllo interno previste nella presente Parte Speciale, i seguenti soggetti esterni (di seguito i "Soggetti Esterni"):

- i consulenti, gli altri collaboratori esterni e, in generale, tutti i soggetti che svolgono attività di lavoro autonomo nella misura in cui essi operino nell'ambito delle aree di attività a rischio per conto o nell'interesse della Società;
- i fornitori e i partner (anche sotto forma di RTI, joint-venture etc.) che operano in maniera rilevante e/o continuativa nell'ambito delle aree di attività a rischio per conto o nell'interesse della Società;
- tutti coloro che, più in generale, a qualunque titolo, operano nell'ambito delle attività a rischio a nome o per conto della Società.

La presente Parte Speciale del Modello ha l'obiettivo di indirizzare, mediante regole di condotta, le attività a rischio poste in essere dai Destinatari **al fine di prevenire il verificarsi dei delitti informatici e di trattamento illecito dei dati di cui all'art. 24 bis del D.Lgs. 231/2001, nonché dei delitti in materia di violazione del diritto d'autore di cui all'art. 25 novies del D.Lgs. 231/2001.**

Nello specifico, essa ha lo scopo di:

- illustrare le **fattispecie di reato** riconducibili alle tipologie dei reati sopraindicati;
- identificare le **attività a rischio** ossia quelle attività che la Società pone in essere, in corrispondenza delle quali, secondo un approccio di *risk assessment*, la Società stessa ritiene inerenti e rilevanti i rischi-reato, riprendendo il contenuto della "*matrice delle attività a rischio*", nella quale, per ciascuna funzione, sono state individuate dai relativi responsabili le attività a rischio. Detto documento forma parte integrante di tutte le Parti Speciali del Modello;
- identificare i **protocolli di comportamento** (riepilogo, integrazione e/o specificazione delle norme comportamentali del Codice Etico di rilievo, nonché obblighi e divieti che i Destinatari sono tenuti ad osservare per una corretta applicazione della presente Parte Speciale del Modello;
- **fornire all'Organismo di Vigilanza e al RPCT gli strumenti operativi** per esercitare le necessarie attività di controllo, monitoraggio e di verifica.

I delitti informatici e il trattamento illecito dei dati di cui all'art. 24 bis del D. Lgs. n. 231/01

Le fattispecie di reato ex art. 24 bis del D.Lgs. 231/2001

L'articolo 24 bis del D.Lgs. 231/2001, inserito dall'art. 7 della L. 18 marzo 2008, n. 48 **e** rubricato "Delitti informatici e trattamento illecito dei dati" così recita:

> *1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.*
> *2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.*
> *3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.*
> *4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).*

In conformità a quanto disposto nella Parte Generale del presente Modello, con riferimento ai seguenti reati:

- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)
- Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies)
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)

si è ritenuto che la specifica attività svolta dalla Società non presenti affatto profili di rischio, o non presenti profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio della stessa.

Al riguardo, si ritiene pertanto esaustivo il richiamo ai principi contenuti nel Codice Etico, nella Parte Generale, nonché ai principi e ai protocolli comunque richiamati dalla presente Parte Speciale e dalle altre Parti speciali che vincolano i Destinatari del Modello.

Gli altri reati richiamati dall'art. 24 bis del Decreto, ivi compresi quelli previsti dagli artt. 476 e seguenti c.p. in relazione all'art. 491 bis c.p. (Documenti Informatici) sono invece stati ritenuti rilevanti, e sono i seguenti:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.)
- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.)
- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.)

- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.)
- Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative (art. 480 c.p.)
- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.)
- Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.)
- Falsità in registri e notificazioni [sotto forma di documento informatico avente efficacia probatoria] (art. 484 c.p.)
- Falsità in scrittura privata (art. 485 c.p.)
- Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.)
- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.)
- Altre falsità in foglio firmato in bianco (art. 488 c.p.)
- Uso di atto falso (art. 489 c.p.)
- Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.)
- 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.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 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.)

Qui di seguito viene pertanto riportato il contenuto letterale degli articoli del codice riguardante le fattispecie di falsità in documento informatico, per facilitare la comprensione di ciascuna fattispecie:

Art. 476 codice penale. Falsità materiale commessa dal pubblico ufficiale
Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni.
Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.

Art. 477 codice penale. Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative
Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni.

Articolo 478 codice penale. Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti
Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni.

Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni.
Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni.

Articolo 479 codice penale. Falsità ideologica commessa dal pubblico ufficiale in atti pubblici
Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476.

Articolo 480 codice penale. Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative
Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni.

Articolo 481 codice penale. Falsità ideologica in certificati commessa da persone esercenti
Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00.
Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro.

Articolo 483 codice penale. Falsità ideologica commessa dal privato in atto pubblico
Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni.
Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi.

Articolo 484 codice penale. Falsità in registri e notificazioni
Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00.

Articolo 485 codice penale. Falsità in scrittura privata *
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni.
Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata.

Articolo 486 codice penale. Falsità in foglio firmato in bianco. Atto privato *
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni.

Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito.

Articolo 487 codice penale. Falsità in foglio firmato in bianco
Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480.

Articolo 488 codice penale. Altre falsità in foglio firmato in bianco
Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dall'art. 487, si applicano le disposizioni sulle falsità materiali in atti pubblici.

Articolo 489 codice penale. Uso di atto falso
Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo.

Articolo 490 codice penale. Soppressione, distruzione e occultamento di atti veri
Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero, o, al fine di recare a sé o ad altri un vantaggio o di recare ad altri un danno, distrugge, sopprime od occulta un testamento olografo, una cambiale o un altro titolo di credito trasmissibile per girata o al portatore veri, soggiace rispettivamente alle pene stabilite negli articoli 476, 477 e 482, secondo le distinzioni in essi contenute.

(*) Innanzitutto appare opportuno rilevare che gli articoli 485 e 486 c.p. sono stati abrogati rispettivamente dall'art. 1 c. 1 lett. a) e lett. b) del D.Lgs. n. 7/2016 e le ipotesi ivi previste, non più penalmente rilevanti, sono state trasformate in illeciti civili sottoposti a sanzioni pecuniarie.
L'art. 4 c. 4 del citato decreto prevede l'applicazione della sanzione pecuniaria civile da euro duecento a euro dodicimila nei confronti di chi:
a) facendo uso o lasciando che altri faccia uso di una scrittura privata da lui falsamente formata o da lui alterata, arreca ad altri un danno. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata;
b) abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facolta' di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, se dal fatto di farne uso o di lasciare che se ne faccia uso, deriva un danno ad altri.

Poiché tuttavia le fattispecie in questione, pur avendo perso rilevanza penale, non sono per ciò stesso considerate dal legislatore condotte giuridicamente lecite, si ritiene preferibile continuare a gestire il rischio che all'interno della Società vengano poste in essere siffatte condotte. Permangono infatti, come detto, profili di illegittimità sotto il profilo civilistico, giacché tali condotte sono soggette all'applicazione di una sanzione pecuniaria civile.
Le fattispecie (dall'art. 476 c.p all'art.490 c.p.) richiamate in modo esplicito dall'art. 491 bis c.p. riguardano i reati di falso nei documenti informatici.

In particolare, il bene giuridico tutelato, dalle fattispecie di reato di cui al capo III del titolo VII del codice penale, è la **fede pubblica** documentale, si tratta di quella particolare fiducia che la collettività ripone sulla veridicità o autenticità di un documento.

Per documento informatico si intende qualsiasi rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; i documenti informatici rilevanti ai fini delle norme in questione sono quelli pubblici aventi efficacia probatoria, cioè con firma elettronica qualificata o emessi nel rispetto di quelle regole tecniche finalizzate a garantirne paternità, provenienza, integrità e immodificabilità.
Può trattarsi di qualunque atto scritto, file o altro contenuto di un programma informatico, del quale sia riconoscibile l'autore che in esso si palesa, contenente una dichiarazione di scienza (esposizione di dati o fatti) o manifestazioni di volontà.
I reati di falso possono avere ad oggetto un atto pubblico oppure una scrittura privata.
Le copie autentiche degli atti pubblici e delle scritture private sono equiparate agli originali quando, a norma di legge, tengano luogo degli originali mancanti.
I testamenti olografi, le cambiali e gli altri titoli di credito trasmissibili per girata o al portatore sono equiparati, ai fini della pena, agli atti pubblici.
La nozione di atto pubblico, ai fini della tutela penale, è certamente più ampia di quella del codice civile, poiché sono ricompresi non solo i documenti redatti con le debite formalità prescritte dalla legge da un notaio o da un pubblico ufficiale autorizzato ad attribuire pubblica fede al documento, ma vi sono ricompresi tutti i documenti formati da un pubblico ufficiale o da un pubblico impiegato o incaricato di un pubblico servizio e compilato, con le formalità previste dalla legge, al fine di comprovare un fatto giuridico o al fine di attestare fatti da lui compiuti o avvenuti in sua presenza e destinato ad assumere rilevanza giuridica.
La nozione di pubblico ufficiale, incaricato di pubblico servizio ed esercente di un servizio di pubblica necessità sono contenute rispettivamente negli artt. 357, 358 e 359 c.p.
E' pubblico ufficiale colui che esercita una pubblica funzione legislativa, giudiziaria o amministrativa. Le prime due attività sono riconducibili rispettivamente alla produzione di norme e all'esercizio della funzione giurisdizionale (non solo i magistrati, ma anche altri soggetti chiamati a svolgere determinate funzioni, come ausiliari, periti, testimoni etc.). L'attività amministrativa è, invece, quella caratterizzata da una regolamentazione pubblicistica, dalla formazione e manifestazione della volontà della pubblica amministrazione e ha ad oggetto l'esercizio di poteri autoritativi, di certificazione e attestazione e documentazione di attività giuridicamente rilevante.
E' incaricato di pubblico servizio, invece, colui che presta, a qualunque titolo, un servizio pubblico, cioè un'attività diretta a soddisfare finalità pubbliche di utilità sociale, caratterizzata da una disciplina di tipo pubblicistico e dall'assenza dei poteri autoritativi tipici di quest'ultima, da un lato, e dall'esclusione di attività non discrezionali, di mera esecuzione di compiti impartiti dall'autorità e di prestazione di opera meramente materiale, dall'altro.
L'esercente di un servizio di pubblica necessità è il privato che, qualora non rientri nelle prime due categorie, eserciti una professione, sanitaria, forense o altra professione per cui è necessaria una particolare abilitazione pubblica, ovvero il privato chiamato a svolgere un servizio dichiarato di pubblica necessità mediante un atto della pubblica amministrazione.
Occorre sottolineare che i reati di cui al capo III del titolo VII del codice penale si possono distinguere a seconda che vengano commessi da soggetti che rivestano una particolare qualifica (c.d. reati propri) ovvero da chiunque (c. d. reati comuni) nel modo seguente:

1. Falsità commesse da pubblico ufficiale o da impiegato incaricato di pubblico servizio (reati propri):
    - **materiale** in atti pubblici (art. 476c.p., con pena aggravata se è atto fidefacente), in certificati o autorizzazioni (art. 477 c.p.), in copie autentiche o attestati (art. 478 c.p.);
    - **ideologica** in atti pubblici (art. 479 c.p.), in certificati o autorizzazioni (art. 480 c.p.)
2. Falsità commesse dal privato (reati comuni):
    - **materiale** in atti pubblici, in certificati, o autorizzazioni, in copie autentiche o attestati (art. 482 c.p., con riduzione di un terzo delle pene rispetto al fatto commesso da un pubblico ufficiale);

- **ideologica** in atti pubblici (art. 483 c.p.).

È doveroso sottolineare tuttavia che anche un soggetto che non riveste le qualifiche richieste per la commissione dei reati propri può commettere il reato in concorso con il pubblico ufficiale o l'incaricato di un pubblico servizio.

Nei casi di condanna per uno dei delitti di falso indicati dall'art. 491 bis c.p., si applica all'ente una sanzione pecuniaria fino a 400 quote e le seguenti sanzioni interdittive: divieto di contrarre con la P.A.; l'esclusione da agevolazioni finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi oltreché il divieto di pubblicizzare beni o servizi.

L'art. 24 bis del Decreto contempla, come sopra evidenziato, altre ipotesi di delitti informatici dei quali qui di seguito viene riportato il contenuto letterale degli articoli, per facilitare la comprensione di ciascuna fattispecie:

(Art. 615 ter c.p.) Accesso abusivo ad un sistema informatico o telematico
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

(Art. 615 quater c.p.) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a € 5.164,00.
La pena è della reclusione da uno a due anni e della multa da € 5.164,00 a € 10.329,00 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

(Art. 617 quater c.p.) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.
Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

(Art. 635 bis c.p.) Danneggiamento di informazioni, dati e programmi informatici
Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

(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
Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

(Art. 635 quater c.p.) Danneggiamento di sistemi informatici o telematici
Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

(Art. 635 quinquies c.p.) Danneggiamento di sistemi informatici o telematici di pubblica utilità
Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Per quanto attiene ai sopraindicati reati informatici, occorre precisare che i beni o interessi giuridici tutelati dalle norme incriminatrici consistono fondamentalmente nella integrità del patrimonio e dei

sistemi informatici, nel corretto funzionamento delle apparecchiature informatiche e telematiche, nonché nella integrità e riservatezza delle informazioni contenute nei sistemi informatici e di quelle trasmesse per via telematica, e vengono presi in considerazione non solo i sistemi informatici complessi ma anche i singoli personal computer.
Nei casi di condanna per uno dei reati informatici in senso stretto le sanzioni pecuniarie sono comprese tra 100 e 500 quote e si applicano le seguenti sanzioni interdittive: sospensione o revoca delle autorizzazioni licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi e nei casi più gravi (artt. 615 ter, 617 quater e quinquies, 635 bis, ter, quater, quinquies c.p.) si giunge fino alla interdizione dall'esercizio dell'attività.

Le fattispecie di reato ex articolo 25 novies del D.Lgs. 231/2001

L'articolo 25 novies del Decreto, introdotto dall'art. 15 c. 7 lett. c) della L. 23 luglio 2009, n. 39 e rubricato "*Delitti in materia di violazione del diritto d'autore*", così recita:
1. In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.
2. Nel caso di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore ad un anno. Resta fermo quanto previsto dall'articolo 174-quinquies della citata legge n. 633 del 1941.

Le fattispecie alle quali fa riferimento l'articolo in esame, in materia di violazione del diritto d'autore, sono:

- Art. 171 c. 1 lett. a-bis) e c. 3 della L. 22 aprile 1941, n. 633
- Art. 171 ter della L. 22 aprile 1941, n. 633
- Art. 171 septies della L. 22 aprile 1941, n. 633
- Art. 171 octies della L. 22 aprile 1941, n. 633

Per quanto concerne tali ipotesi di reato, riguardanti le opere dell'ingegno in genere, letterarie, musicali, arti figurative, cinematografiche, fotografiche, teatrali etc., si richiamano le osservazioni contenute nella Parte Generale del Modello e si ribadisce che l'attività svolta dalla Società non presenta, in relazione alle predette fattispecie di reato, profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio della stessa, mentre è rilevante e viene analizzata e gestita l'ipotesi di cui all'art. art. 171 bis della L. 22 aprile 1941, n. 633, di cui di seguito si riporta il contenuto letterale:

Art. 171 bis della L. 22 aprile 1941, n. 633
Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da € 2.582,00 a € 15.493,00. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a € 15.493,00 se il fatto è di rilevante gravità.

Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64 quinquies e 64 sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102 bis e 102 ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto, alla pena della reclusione da sei mesi a tre anni e della multa da € 2.582,00 a € 15.493,00. La pena non è inferiore nel minimo a due anni di reclusione e la multa a € 15.493,00 se il fatto è di rilevante gravità.

L'art. 171 bis riguarda le condotte di duplicazione abusiva, importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale, e locazione, per trarne profitto, di programmi per elaboratore contenuti in supporti non contrassegnati SIAE, ovvero l'utilizzo di mezzi atti a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione dei programmi medesimi.
Al secondo comma, invece, sono previste le condotte di illegittima riproduzione, illegittimo trasferimento su altro supporto, illegittima distribuzione, illegittima comunicazione, illegittima presentazione o dimostrazione in pubblico, al fine di trarne profitto, del contenuto di una banca dati, ovvero l'illegittima estrazione o reimpiego illegittimo, illegittima distribuzione, illegittima vendita e illegittima locazione della stessa.

L'art. 25 novies del Decreto, prevede non solo sanzioni pecuniare, ma anche le seguenti sanzioni interdittive per una durata non inferiore ad un anno: interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.

Le macroattività a rischio ex artt. 24 bis e 25 novies del D.Lgs. n. 231/2001

Con riferimento al rischio di commissione dei reati illustrati nei paragrafi precedenti (di cui agli articoli 24 bis e 25 novies del D.Lgs. 231/2001) e ritenuti rilevanti a seguito del *risk assessment* eseguito internamente, la Società valuta come "a rischio" le seguenti macroattività che essa pone in essere per mezzo dei Destinatari della presente Parte Speciale anche eventualmente in collaborazione con i Soggetti Esterni:

1) Rilascio di certificati, autorizzazioni, attestati, o documenti di analogo contenuto, di copie conformi, e di atti in genere da parte di un p.u. o di un i.p.s. e relativa richiesta; utilizzo dei predetti documenti, ivi compresa la trasmissione telematica;
2) Dichiarazioni rilasciate ad un p.u. o i.p.s.;
3) Formazione e utilizzo, ivi compresa la trasmissione telematica, di scritture private, di corrispondenza;
4) Atti compiuti dal medico competente o altro esercente professione sanitaria;
5) Gestione registri carico/scarico;
6) Denuncia infortuni all'Autorità di P.S.;
7) Rilascio di procure speciali e autenticazione sottoscrizione da parte di un esercente della professione forense;

8) Attività di creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici in entrata e in uscita e manutenzione in genere degli archivi di documenti informatici;
9) Comunicazioni interne sotto forma di documento informatico;
10) Utilizzo dei sistemi informatici e telematici aziendali;
11) Gestione delle attività di accesso ai sistemi informatici/telematici e applicazioni (credenziali, attività di autenticazione e accesso, definizione account e profili etc.);
12) Gestione e manutenzione hardware;
13) Installazione, gestione e manutenzione software;
14) Installazione, accesso e utilizzo banche dati.

Le macroattività a rischio come sopra identificate, sono meglio specificate, funzione per funzione, nella "*matrice delle attività a rischio*", fatta salva l'integrazione delle stesse in fase di implementazione, nonché, in divenire, ad opera dell'OdV o delle singole funzioni in collaborazione con l'OdV medesimo.

I reati ex art. 24 bis e 25 novies del D.Lgs. 231/2001 – Protocolli comportamentali

Ai fini dell'attuazione delle regole comportamentali e dei divieti di seguito elencati, i Destinatari della presente Parte Speciale del Modello, oltre a rispettare le previsioni di legge esistenti in materia, le norme e i principi contenuti nel Codice Etico e nella Parte Generale del presente Modello, nonché le misure di prevenzione di fenomeni corruttivi in senso ampio (maladministration) contenute nel Piano triennale di prevenzione della corruzione adottato dalla Società, devono rispettare i protocolli comportamentali di seguito descritti, posti a presidio dei rischi-reato sopra identificati e riferibili alle attività a rischio.
I protocolli comportamentali prevedono obblighi e/o divieti specifici che i Destinatari della presente Parte Speciale del Modello devono rispettare, uniformando la propria condotta ad essi in corrispondenza delle attività a rischio sopra rilevate. Tali principi riprendono, specificandolo o, se necessario, integrandolo, il contenuto del Codice Etico e della Parte Generale del Modello. In forza di apposite pattuizioni contrattuali, i principi in esame si applicano anche ai Soggetti Esterni coinvolti nello svolgimento delle attività a rischio identificate.

In particolare, costituisce un preciso obbligo per la Società ricorrere alla formulazione di quesiti o alla richiesta di pareri alla Pubblica Amministrazione interessata o all'Autorità pubblica alla quale sia demandata attività di vigilanza e controllo, o comunque competente per materia, o ad un professionista esterno prima del compimento di un atto o dello svolgimento di un'attività, ogniqualvolta vi siano dubbi sull'interpretazione o applicazione di una norma giuridica ovvero sulla qualificazione giuridica di un fatto o di un atto.

OBBLIGHI

Tutte le attività a rischio devono essere svolte conformandosi alle leggi vigenti, alle norme e ai principi contenuti nel Codice Etico, alle norme e ai principi generali di comportamento enucleati sia nella Parte Generale che nella Parte Speciale del presente Modello, nonché ai protocolli comportamentali che seguono, posti a presidio dei rischi-reato identificati.

La Società:

- definisce i requisiti di autenticazione e di accesso ai sistemi informatici/telematici utilizzati, con particolare riferimento a quelli della Pubblica Amministrazione o comunque di pubblica utilità, alle applicazioni e alle banche dati (regole per la creazione, attribuzione, modifica, conservazione di password, assegnazione di adeguati livelli di privilegio e relativa ssunzione di reponsabilità);
- provvede affinché vengano generati, protetti e conservati i "log" di accesso;
- provvede all'installazione, gestione e manutenzione dell'hardware aziendale, inventario compreso;
- provvede all'implementazione di misure protettive del sistema da accessi non autorizzati dall'esterno (antivirus, firewall etc.);
- provvede alle attività di backup periodico e all'adozione di soluzioni di disaster recovery e di business continuity;
- provvede alla regolamentazione degli accessi fisici al luogo in cui è posizionato il server e le altre infrastrutture IT.
- provvede all'installazione, gestione e manutenzione del software e delle banche dati (ivi compresi inventario, verifica di validità, operatività, scadenza e limiti di licenze e certificazioni di software e banche dati di terzi o loro utilizzo in conformità alle norme sul diritto d'autore e altri diritti connessi al suo esercizio; divieti o limitazioni di installazione/utilizzo) al fine di garantire che:
    - venga installato/utilizzato solo software con licenza d'uso e nei limiti ed alle condizioni previste dalla normativa vigente e dalla licenza medesima, ad eccezione di quei programmi per elaboratore disponibili per il download e utilizzo libero, sempre alle condizioni e nei limiti previsti dalla legge o dal titolare del diritto d'autore e degli altri diritti connessi al suo utilizzo;
    - vengano installate/utilizzate solo banche dati con licenza d'uso e nei limiti ed alle condizioni previste dalla normativa vigente e dalla licenza medesima ad eccezione di quelle liberamente consultabili, sempre alle condizioni e nei limiti previsti dalla legge o dal titolare del diritto d'autore e degli altri diritti connessi al suo utilizzo, anche per quanto attiene alla ricerca, estrazione, elaborazione, rielaborazione e pubblicazione dei dati ivi contenuti.
- regolamenta l'utilizzo di dispositivi elettronici personali per finalità aziendali e di quelli aziendali per finalità ad essa estranee;
- regolamenta l'accesso a siti internet da sistemi aziendali o con connessione aziendale, disponendo le opportune restrizioni di navigazione al fine di evitare che questa avvenga per finalità non aziendali (ivi compresa la frequentazione di siti con contenuti pornografici e il download del materiale ivi contenuto);
- regolamenta l'utilizzo della posta elettronica aziendale, degli indirizzi di posta elettronica personali per l'attività aziendale, nonché dei software di gestione della posta;
- provvede affinché nei processi di creazione, protezione, emissione, ricezione, archiviazione, conservazione, eliminazione, immissione in reti informatiche/telematiche di documenti informatici vengano adottate precauzioni idonee a garantire la provenienza, l'integrità e l'immodificabilità dei documenti medesimi.
- regolamenta l'utilizzo della firma digitale con formale attribuzione e formale assunzione della relativa responsabilità.
- provvede alla nomina di amministratore/i di sistema e amministratore di rete, con un atto formale, definendo compiti e attribuzioni ed espressa assunzione della relativa responsabilità;

Per quanto attiene alla sicurezza dei dati personali di tutti i soggetti con i quali intrattiene rapporti a vario titolo, la Società ha adeguato il suo sistema organizzativo ai principi e obblighi di cui alla normativa vigente in materia e, in particolare, del **Decreto legislativo 30 giugno 2003, n. 196** (Codice in materia di protezione dei dati personali), e garantisce che il trattamento dei dati medesimi si svolge nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

DIVIETI

E' fatto espresso divieto ai Destinatari di porre in essere comportamenti tali da integrare, anche solo potenzialmente e anche a titolo di concorso o di tentativo, le fattispecie di reato di cui alla presente Parte Speciale.

In particolare, premesso che:

- ✓ la definizione di "concorso" di persone del reato data dal codice penale ricomprende nel "contributo obiettivamente rilevante" ogni forma di collaborazione, anche "morale", idonea, cioè, determinare o a rafforzare il proposito criminoso di altri soggetti (e.g. istigazione),
- ✓ per documento informatico deve intendersi qualsiasi rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, di natura pubblica, qualora dotato di "efficacia probatoria", cioè con firma elettronica qualificata o emesso nel rispetto di quelle regole tecniche finalizzate a garantirne paternità, provenienza, integrità e immodificabilità,

ai Destinatari è fatto divieto di:

- Formare o concorrere con un pubblico ufficiale o incaricato di pubblico servizio a formare documenti informatici falsi o alterare atti veri;
- Contraffare o alterare o concorrere con un p.u. o i.p.s. nel contraffare o alterare certificati o autorizzazioni amministrative contenute in un documento informatico, o a contraffare o alterare le condizioni richieste per la loro validità;
- Concorrere con un p.u. o i.p.s. a formare e rilasciare una copia in forma legale su documento informatico di un atto pubblico o privato inesistente o una copia diversa dall'originale.
- Contraffare o concorrere con un p.u. o i.p.s. nel contraffare un attestato.
- Concorrere con un p.u. o i.p.s. nella falsa attestazione da parte di quest'ultimo in un documento informatico che un fatto è stato da lui compiuto o che è avvenuto in sua presenza, ovvero nell'attestazione da parte dello stesso in un documento informatico di aver ricevuto dichiarazioni non rese o nell'omissione o alterazione di dichiarazioni da lui ricevute;
- Concorrere con un p.u. o i.p.s. nella falsa attestazione, in atti, in certificati o autorizzazioni amministrative sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità.
- Concorrere con un esercente una professione sanitaria o forense o altro servizio di pubblica necessità nell'attestare falsamente, in un certificato sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità.
- Attestare falsamente, oralmente o per iscritto, ad un p.u. in un atto pubblico, sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità.
- Formare in tutto o in parte scritture private false, sotto forma di documento informatico, o alterazione di scritture private vere, utilizzandole o lasciando che altri le utilizzino.

- Scrivere o far scrivere, su documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto privato produttivo di effetti giuridici diversi da quelli previsti, utilizzandolo o lasciando che altri lo utilizzino.
- Scrivere o far scrivere, ovvero concorrere con un p.u. nello scrivere o nel far scrivere, su documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto pubblico diverso da quello a cui il p.u. stesso era obbligato o autorizzato.
- Distruggere, sopprimere, occultare in tutto o in parte una scrittura privata o un atto pubblico veri, sotto forma di documento informatico.
- Utilizzare abusivamente la firma digitale aziendale o, comunque, in violazione delle procedure che ne regolamentano l'utilizzo.
- Duplicare abusivamente, detenere o installare programmi per elaboratore contenuti in supporti non contrassegnati SIAE o senza regolare licenza, o comunque utilizzarli non rispettando le condizioni o i limiti previsti dalla legge, dalla licenza, o dal titolare del diritto d'autore e degli altri diritti connessi al suo utilizzo;
- Installare o utilizzare banche dati senza licenza d'uso o non rispettando limiti e condizioni previsti dalla legge, dalla licenza o dal titolare del diritto d'autore e degli altri diritti connessi al suo utilizzo, anche per quanto attiene alla ricerca, estrazione, elaborazione, rielaborazione e pubblicazione dei dati ivi contenuti;
- Introdursi abusivamente o permanere contro la volontà espressa o tacita dell'avente diritto, in un sistema informatico o telematico protetto da misure di sicurezza;
- Intercettare, ovvero acquisire illegittima conoscenza di comunicazioni telematiche[1], impedire o interrompere comunicazioni telematiche, ovvero frapporre ostacoli hardware o software all'utilizzo di un sistema informatico o telematico, affinché una comunicazione telematica non giunga a destinazione o giunga a destinazione con contenuto alterato;
- Rivelare al pubblico, ovvero portare illegittimamente a conoscenza di terzi, il contenuto di documenti informatici destinati a rimanere segreti o riservati.
- Procurarsi, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo;
- Distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui, o utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- Distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici altrui, ovvero ostacolarne gravemente il funzionamento mediante distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici altrui o attraverso l'introduzione o la trasmissione di dati, informazioni o programmi;
- Distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o introduzione o trasmissione di dati, informazioni o programmi al fine distruggere, danneggiare, o causare l'inutilizzabilità in tutto o in parte di sistemi informatici o telematici ovvero al fine di ostacolarne gravemente il loro funzionamento.

Sistema di deleghe e procure

Il sistema di deleghe e procure concorre insieme agli altri strumenti del presente Modello ai fini della prevenzione dei rischi-reato nell'ambito delle attività a rischio identificate.

[1] N.B: anche l'invio di e-mail è considerata a tutti gli effetti una comunicazione telematica

La “procura” è il negozio giuridico unilaterale con cui la Società attribuisce poteri di rappresentanza nei confronti dei terzi.

Per “delega” si intende qualsiasi atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative.

Tutte le risorse, per lo svolgimento dei loro incarichi, sono munite di “procura funzionale” o “delega” formalizzate, scritte ed espressamente accettate, di estensione adeguata e coerente con le funzioni, che definiscono le responsabilità e i poteri attribuiti. Tutte le procure e deleghe conferite fissano espressamente per natura e/o limite di importo, l’estensione dei poteri di rappresentanza o di quelli delegati.

Riguardo alle attività a rischio, l’Organo amministrativo ha l’onere di assicurare che tutti coloro (i Destinatari e eventualmente anche i Soggetti Esterni) che agiscono per conto della Società e, soprattutto, che impegnano legalmente la Società, siano dotati di apposita procura o delega.

Le procure e le deleghe devono trasferire attribuzioni, poteri e responsabilità nei limiti previsti dalle norme giuridiche vigenti e applicabili e, in particolare, non devono violare disposizioni normative inderogabili; devono essere coerenti con il Sistema di Controllo Interno, con il Codice Etico e con il Modello; definiscono in modo specifico ed inequivoco i poteri del procuratore o del delegato e il soggetto cui quest’ultimo riporta. I poteri gestionali assegnati e la loro attuazione sono coerenti con gli obiettivi aziendali e la struttura organizzativa della Società.

La Società, mediante organigramma o comunicazioni organizzative adeguatamente divulgate al suo interno, definisce:

- delimitazione dei ruoli, descrizione dei compiti di ciascuna funzione e dei relativi attribuzioni e poteri;
- descrizione delle linee di riporto.

Procedure e regolamentazione flussi informativi in favore di OdV e RPCT

Al fine di avere gli strumenti per esercitare le sue attività di monitoraggio e di verifica puntuale della efficace esecuzione protocolli previsti dal presente Modello e, in particolare, dalla presente Parte Speciale, la Società definisce, implementa e diffonde specifiche policies aziendali, un organigramma contenente gli ambiti e le responsabilità di ciascuna funzione, nonché regolamenti interni o procedure dettagliate e specifiche (eventualmente integrando quelle che verranno implementate nell’ambito del sistema di gestione della qualità dell’organizzazione, di gestione ambientale e della sicurezza dei lavoratori, basato sulle norme UNI EN ISO 9001:2008, UNI EN ISO 14001:2004 e OHSAS 18001:2007) che andranno a guidare e regolamentare lo svolgimento delle attività sensibili considerate, e di quelle ad esse strumentali o comunque collegate, nonché per i relativi controlli, definendo in dettaglio il sistema di riporto e i flussi informativi nei confronti del RPCT e dell’OdV, in conformità a quanto disposto nella Parte Generale del Modello.

In particolare, le procedure devono garantire:

- conformità ai Principi enunciati nel Codice Etico e nella Parte Generale del Modello;
- conformità ai protocolli comportamentali individuati nella presente Parte Speciale;
- chiarezza e precisione dei vari ruoli, compiti, attribuzioni, poteri e responsabilità;
- l’individuazione di un responsabile per ciascuna attività sensibile o per ciascuna fase della stessa;

- chiarezza e precisione delle varie linee di riporto;
- segregazione delle funzioni (separazione per ciascun processo tra il soggetto che decide, quello che autorizza, quello che esegue e quello che controlla);
- tracciabilità di tutte le fasi del processo e dei relativi soggetti;
- adeguati controlli (preventivi, concomitanti o successivi; automatici o manuali; continui o periodici; analitici o a campione), di tutte le fasi critiche del processo;
- flussi informativi nei confronti dell'OdV e del RPCT.

E' comunque fatto salvo per tutti i Destinatari l'obbligo di comunicare all'OdV e al RPCT qualsiasi anomalia, difformità, irregolarità, deroga o altro fatto "significativo" attinente allo svolgimento di attività a rischio, anche se lo stesso non dovesse integrare propriamente una violazione del Modello.

La presente Parte Speciale è stata approvata e adottata dal Consiglio di Amministrazione della Villaservice S.p.a. con delibera del 29 marzo 2021