Organizzazione

Digitronica.IT S.p.A.
Sede: Viale del Lavoro, 52 Verona
Phone: 045 50 19 01
Fax: 045 50 22 58
Email: info@digitronica.it
Pec: digitronica.it@pec.it

MOGC 231 – PARTE SPECIALE

ai sensi del D.Lgs. n. **231** del 8 Giugno 2001 e s.m.i.

Master	☐
Copia controllata	☐
Copia non controllata	☐
Numero della copia	☐

Emissione DG	Data		Firma	
Approvazione DG	Data		Firma	
Approvazione ODV	Data		Firma	

Stato delle revisioni

Versione	Data	Descrizione	Autore
00	*04/06/2019*	Prima emissione	Digitronica.IT Srl
01	*01/12/2020*	Aggiornamento	Digitronica.IT S.p.A.
02	*01/04/2022*	Aggiornamento	Digitronica.IT S.p.A.
03	*22/01/2024*	Aggiornamento OdV	Digitronica.IT SpA

Indice generale della sezione

Modello di Organizzazione, Gestione e Controllo – Parte speciale

2 - Finalità della parte speciale

La Parte Speciale ha la finalità di definire linee, regole e principi di comportamento che tutti i destinatari del Modello 231 dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività sensibili svolte nella società, la commissione di reati previsti dal Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la Parte Speciale del Modello 231 ha lo scopo di:

- Indicare le modalità che gli esponenti aziendali sono chiamati ad osservare ai fini della corretta applicazione del Modello
- Fornire all'OdV ed alle altre funzioni di controlli gli strumenti per esercitare le attività di monitoraggio, controllo e verifica

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi ai contenuti dei seguenti documenti:

- Modello 231
- Codice Etico
- Procedure e disposizioni
- Procure e deleghe
- Ordini di servizio
- Comunicazioni organizzative
- Sistemi di gestione delle problematiche di sicurezza e ambientali
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.

2.1 - Struttura della parte speciale

La presente Parte Speciale è composta da una parte preliminare dedicata alle regole generali cui si uniforma la condotta degli organi sociali, dei dipendenti, dei partners commerciali, dei collaboratori o consulenti e dei soggetti esterni che operano in nome e per conto dell'azienda (qui di seguito, per brevità, semplicemente "destinatari del Modello 231") ed all'individuazione delle aree di attività a rischio, nonché da singole sezioni dedicate alle categorie di reati presi in considerazione dal Decreto e considerate sensibili dalla società a seguito di *gap-analisys*.
Le sezioni della Parte Speciale sono le seguenti.

SEZIONE "A"	Reati societari Art. 25-ter D.Lgs. 231/01
SEZIONE "B"	Reati di omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro Art. 25-septies D.Lgs. 231/01
SEZIONE "C"	Delitti informatici e trattamento illecito di dati Art. 24-bis D.Lgs. 231/01

Ad integrazione del Modello 231 sono annessi alla presente Parte Speciale i manuali e le procedure di sistemi di gestione integrata ISO 9001 e ISO 27001.

A seguito dell'aggiornamento generale del Modello, effettuato nel Dicembre 2020, la Società ha ritenuto di inserire, all'interno dei reati presupposto della Parte Speciale, anche la sezione:

SEZIONE "D"	Reati tributari Art. 25-quinquiedecies D.Lgs. 231/01

A seguito dell'aggiornamento generale del Modello, effettuato nell'Aprile 2022, la Società ha ritenuto di inserire, all'interno dei reati presupposto della Parte Speciale, anche la sezione:

SEZIONE "E"	Reati contro la Pubblica Amministrazione Artt. 24 e 25 D.Lgs. 231/01
SEZIONE "F"	Delitti in materia di strumenti di pagamento diversi dai contanti Art. 25 octies.1 D. Lgs. 231/01

2.2 - Specifiche circa i delitti tentati

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti rilevanti ai fini della responsabilità amministrativa degli enti, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 del d.lgs. 231/2001). L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra ente e soggetti che assumono di agire in suo nome e per suo conto.

Si tratta di un'ipotesi particolare del c.d. "recesso attivo", previsto dall'art. 56, comma 4, c.p..

- [x] **Sistema di gestione**
- [x] *Modello di organizzazione*
- [ ] *Codice etico*
- [ ] *Analisi dei rischi*
- [ ] **Procedure**
- [ ] **Modulistica**

Digitronica.IT
Your Security Our Software

Organizzazione

Digitronica.IT S.p.A.

Sede: Viale del Lavoro, 52 Verona
Phone: 045 50 19 01
Fax: 045 50 22 58
Email: info@digitronica.it
Pec: digitronica.it@pec.it

MOGC 231 – PARTE SPECIALE

ai sensi del D.Lgs. n. **231** del 8 Giugno 2001 e s.m.i.

Master	
Copia controllata	
Copia non controllata	
Numero della copia	

Emissione DG	Data		Firma	
Approvazione DG	Data		Firma	
Approvazione ODV	Data		Firma	

Stato delle revisioni

Versione	Data	Descrizione	Autore
00	*04/06/2019*	Prima emissione	Digitronica.IT Srl
01	*01/12/2020*	Aggiornamento	Digitronica.IT S.p.A.
02	*01/04/2022*	Aggiornamento	Digitronica.IT S.p.A.
03	*22/01/2024*	Aggiornamento OdV	Digitronica.IT SpA

Indice generale della sezione

Modello di Organizzazione, Gestione e Controllo – Parte speciale

3.1 - Introduzione e funzione della parte speciale dedicata ai reati societari

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Dipendenti e dagli Organi Societari dell'azienda, nonché dai suoi Collaboratori esterni e dai suoi Partner, come già definiti nella Parte Generale

Obiettivo della presente Parte Speciale è che tutti i Destinatari, conducano comportamenti conformi a quanto ivi rescritto al fine di impedire il verificarsi degli illeciti di cui all'art. 25-ter del Decreto

Nello specifico, la presente Parte Speciale ha lo scopo di:

- Indicare i principi procedurali e le regole di comportamento che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello
- Fornire all'Organismo di Vigilanza - e ai responsabili delle funzioni aziendali che cooperano con tale organismo - gli strumenti esecutivi per esercitare le attività di controllo, di monitoraggio e di verifica

La società adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione delle fattispecie delittuose di seguito descritte

3.2 - Le fattispecie di reato richiamate dal D.Lgs. 231/01

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D.Lgs. n. 231/2001 è collegato il regime di responsabilità a carico della società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto

L'art. 25-ter del Decreto contempla la maggior parte dei reati societari che costituiscono, al momento, insieme agli abusi di mercato, i soli reati autenticamente economici di cui può essere chiamata a rispondere la Società e che, in quanto non occasionati dall'esercizio della specifica attività aziendale, sono qualificabili come reati generali

Di seguito si riporta una breve descrizione dei reati societari richiamati dall'art. 25-ter (Reati societari) del D.Lgs. 231/01 che si ritiene potrebbero trovare manifestazione nell'ambito delle attività svolte dall'azienda

La presente Parte Speciale si riferisce ai reati societari

3.2.1 - False comunicazioni sociali (Art. 2621, 2621 bis, 2621 ter c.c.)

Questo reato si realizza tramite:

- l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge e dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni idonee ad indurre in errore i destinatari sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, con l'intenzione di ingannare i soci o il pubblico
- l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge

La pena prevista per tale reato **dall'art. 9. della legge n.69 del 27 maggio 2015 che ha modificato l'art. 2621,** è la reclusione da uno a cinque anni

L'art. 10. della legge n.69 del 27 Maggio 2015 introduce gli articoli 2621 bis e ter del codice civile

Art. 2621-bis Fatti di lieve entità
Salvo che costituiscano più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'articolo 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.

Art. 2621-ter Non punibilità per particolare tenuità
Ai fini della non punibilità per particolare tenuità del fatto, di cui all'articolo 131-bis del codice penale, il giudice valuta, in modo prevalente, l'entità dell'eventuale danno cagionato alla società, ai soci o ai creditori conseguente ai fatti di cui agli artt.2621 e 2621bis

Si precisa che:

- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto
- le informazioni false o omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene
- la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi

Esempio
Il Consiglio di Amministrazione ignora l'indicazione all responsabile amministrativo circa l'esigenza di un accantonamento (rettifica) al Fondo svalutazione crediti a fronte della situazione di crisi di un cliente, ed iscrive un ammontare di crediti superiore al dovuto; ciò al fine di non far emergere una perdita che comporterebbe l'assunzione di provvedimenti sul capitale sociale (artt. 2446 e 2447 del codice civile).

3.2.2 - False comunicazioni sociali delle società quotate (Art.2622 c.c.)

Alle società indicate nel comma precedente sono equiparate:

- le società emittenti strumenti finanziari per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea
- le società emittenti strumenti finanziari ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano
- le società che controllano società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea
- le società che fanno appello al pubblico risparmio o che comunque lo gestiscono

Le disposizioni di cui ai commi precedenti si applicano anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi

L'art. 11. della legge n.69 del 27 maggio 2015 sostituisce l'articolo 2622 del codice civile e recita:

Art. 2622 False comunicazioni sociali delle società quotate

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da tre a otto anni

3.2.3 - Impedito controllo (art. 2625 c.c. modificato da D.Lgs n.39 del 27 gennaio 2010)

Il reato consiste nell'impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci, ad altri organi sociali

Il reato è punito con la sanzione amministrativa di 10.329 Euro

Se la condotta ha però cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa.

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

Esempio

Un funzionario della società rifiuta di fornire alla società di revisione i documenti richiesti per l'espletamento dell'incarico, quali, ad esempio, quelli concernenti le azioni legali intraprese dalla società per il recupero di crediti.

3.2.4 - Indebita restituzione dei conferimenti (art. 2626 c.c.)

La "condotta tipica" prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche simulata, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli

La pena prevista è fino ad un anno di reclusione

Esempio

L'Assemblea dell'azienda, su proposta del Consiglio di Amministrazione, delibera la compensazione di un debito di un socio nei confronti della società con il credito da conferimento che quest'ultima vanta nei confronti del socio medesimo, attuando di fatto una restituzione indebita del conferimento.

3.2.5 - Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva; ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite

La pena prevista è fino ad un anno di reclusione

Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato

Esempio

L'Assemblea della Società, su proposta del Consiglio di Amministrazione, delibera la distribuzione di dividendi che costituiscono, non un utile di esercizio, ma fondi non distribuibili perché destinati dalla legge a riserva legale.

3.2.6 - Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)

Questo reato si perfeziona con l'acquisto o la sottoscrizione di azioni o quote sociali della società controllante, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge
La pena prevista è fino ad un anno di reclusione
Si fa presente che se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio, relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto

Esempio

L'Organo amministrativo procede all'acquisto o alla sottoscrizione di azioni della società o di una società controllante fuori dai casi di cui all'artt. 2357, 2359-bis del codice civile, cagionando in tal modo una lesione del patrimonio sociale.

3.2.7 - Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori

Il reato è punito, a querela della persona offesa, da sei mesi a tre anni

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato

Esempio

L'organo amministrativo delibera una riduzione del capitale sociale senza osservare i presupposti richiesti dalla legge, cagionando in tal modo un danno ai creditori sociali.

3.2.8 - Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.)

Il reato si perfeziona nel caso in cui l'amministratore di una società con azioni quotate non comunichi agli altri amministratori e al collegio sindacale un interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società, cagionando a seguito di tale omissione un danno alla società o a terzi

Tale ipotesi di reato non può configurarsi in capo all'azienda se questa non è quotata

Esempio

Un amministratore di una società quotata, nel corso di una riunione del Consiglio di Amministrazione della stessa, convocato per valutare e deliberare un'acquisizione societaria ad un prezzo eccessivo rispetto al reale valore della target, non comunica agli altri consiglieri che sua moglie è proprietaria di una partecipazione di maggioranza nella società oggetto dell'acquisizione

3.2.9 - Formazione fittizia del capitale (art. 2632 c.c.)

Tale ipotesi si ha quando viene formato o aumentato fittiziamente il capitale della società mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; vengono sottoscritte reciprocamente azioni o quote; vengono sopravvalutati in modo rilevante i conferimenti dei beni in natura, i crediti ovvero il patrimonio della società nel caso di trasformazione

Esempio

L'Assemblea dell'azienda, su proposta del Consiglio di Amministrazione, delibera l'aumento del capitale sociale con un conferimento di beni sopravvalutati in modo rilevante.

3.2.10 - Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori

Il reato è punito, a querela della persona offesa, da sei mesi a tre anni

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato

3.2.11 - Corruzione tra privati (art. 2635 c.c. modificato dalla L. n3 del 9 gennaio 2019)

L'art.3 del D.Lgs n. 38 del 15 marzo 2017 recita: «Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni.

Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo

Chi, anche per interposta persona, offre, promette o dà' denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma, è punito con le pene ivi previste

Le pene stabilite sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

La misura della confisca per valore equivalente non può essere inferiore al valore delle utilità date, promesse o offerte

3.2.12 -Istigazione alla corruzione tra privati (art. 2635-bis c.c. modificato dalla L. n3 del 9 gennaio 2019)

Il D.Lgs n. 38 del 15 marzo 2017 con l'art.4 ha introdotto il suddetto reato che recita:
Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.

La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata.

3.2.13 - Pene accessorie (art. 2635-ter c.c.)

Dopo l'articolo 2635-bis l'art.5 del D.Lgs 38 ha inserito l'art. 2635-ter che recita:

La condanna per il reato di cui all'articolo 2635, primo comma, importa in ogni caso l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese di cui all'articolo 32-bis del codice penale nei confronti di chi sia già stato condannato per il medesimo reato o per quello di cui all'articolo 2635-bis, secondo comma.».

3.2.14 - Illecita influenza sull'assemblea (art. 2636 c.c.)

La "condotta tipica" prevede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto

La pena prevista è da sei mesi a tre anni di reclusione

Esempio

Il Consiglio di Amministrazione della società, al fine di ottenere una deliberazione favorevole dell'assemblea e il voto determinante anche del socio di maggioranza, predispone e produce nel corso dell'adunanza assembleare documenti alterati, diretti a far apparire migliore la situazione economica e finanziaria di un'azienda che lo stesso Consiglio di Amministrazione intende acquisire, in modo da ricavarne un indiretto profitto.

3.2.15 - Aggiotaggio (art. 2637 c.c.)

La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di società o gruppi

La pena prevista è da uno a cinque anni di reclusione.

Esempio

Il Direttore Generale dell'azienda diffonde al mercato la notizia del mancato rilascio da parte societaria di una polizza fideiussoria richiesta nell'ambito di un'operazione avente ad oggetto il trasferimento di azioni di una società non quotata. A causa di tale comunicazione il potenziale acquirente rinuncia a concludere il contratto di compravendita dei suddetti titoli.

3.2.16 - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)

La condotta criminosa si realizza attraverso l'esposizione nelle comunicazioni alle autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero con l'occultamento, in tutto o in parte,

con altri mezzi fraudolenti di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima

L'art.101 comma 1 del D.Lgs n.180 del 16 novembre 2015 stabilisce che agli effetti della legge penale, le autorità' e le funzioni di risoluzione di cui al decreto di recepimento della direttiva 2014/59/UE sono equiparate alle autorità e alle funzioni di vigilanza

Esempio
Il Direttore Generale della Società omette di comunicare alla Consob l'acquisizione di una partecipazione rilevante, al fine di evitare possibili controlli dell'autorità di vigilanza.

3.3 - Le attività sensibili relative ai reati societari

L'art. 6, comma 2, lett. a) del D.Lgs. 231/01 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 della società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto

Nell'ambito di ciascun reato, sulla base della mappatura di dettaglio delle aree aziendali a rischio, sono state individuate le attività da ritenersi maggiormente "sensibili" come di seguito riportato.

La società si riserva di aggiornare il presente Modello 231 nel caso in cui dovesse emergere la significatività di uno o più degli altri reati sopra elencati.

Principali Aree a rischio e attività sensibili interessate:

Funzione "Finance & Administration":
- **Imputazione delle scritture contabili** in contabilità generale
- **Verifiche sui dati contabili** immessi a sistema e quelli inviati al consulente esterno
- **Gestione delle comunicazioni verso soci**: si tratta dell'attività di predisposizione della documentazione oggetto di comunicazioni verso soci

Le seguenti attività sensibili vengono svolte dal Consulente esterno – Dottore Commercialista:
- **Predisposizione di bilanci e documentazione di natura contabile**: si tratta delle attività relative alle chiusure contabili, alla contabilizzazione dei dati e alla predisposizione del bilancio d'esercizio della Società e dei relativi allegati
- **Predisposizione di documenti** ai fini delle delibere assembleari e delle decisioni dell'Amministratore Unico: si tratta delle attività di predisposizione della documentazione relativa all'oggetto dell'Assemblea e dell'Amministratore Unico per consentire a questi ultimi di esprimersi sulle materie di propria competenza sottoposte ad approvazione

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

a) degli standard di controllo generali
b) dei principi di comportamento individuati nel Codice Etico
c) di quanto regolamentato dalla documentazione e dagli atti aziendali
d) delle disposizioni di legge

È responsabilità del Legale rappresentante segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche/integrazioni da apportare alla Parte Speciale, in accordo a quanto previsto dalla Parte Generale

3.4 - Organi e funzioni aziendali coinvolte

In relazione alle descritte Attività Sensibili, si ritengono particolarmente coinvolti i seguenti organi e funzioni aziendali nello svolgimento delle proprie attività commerciali, finanziarie, di informazione e di controllo sia in favore della società stessa sia in favore della Clientela

Assemblea dei Soci
I profili di rischio attengono alle funzioni di controllo sulle Aree Sensibili, nonché le attività relative alla gestione dei valori svolte sia per conto della società sia per conto della clientela

Internal audit & Compliance
L'Internal Audit potrebbe presentare il rischio di culpa in vigilando, consistente nel mancato o non corretto controllo delle attività svolte all'interno dell'azienda che coinvolgano le Autorità amministrative

Finance & Administration
L'attività di questa funzione si considera a rischio per la gestione della corretta rappresentazione dei risultati economici, degli adempimenti fiscali

3.5 - Principi e regole di comportamento

Per quanto concerne le fattispecie criminose che si riferiscono ai documenti contabili, si rileva che la società si pone in una posizione privilegiata dal punto di vista della prevenzione e della corretta attuazione dei precetti normativi, in quanto risulta destinataria di una disciplina speciale che impone la procedimentalizzazione dell'intera fase di elaborazione di detta documentazione, nonché una serie di obblighi ed adempimenti in relazione ai rapporti con le autorità, con la conseguenza che le modalità di gestione del rischio dei reati qui considerati risultano replicare comportamenti già consolidati nella prassi societaria o, comunque, derivanti dall'applicazione delle norme primarie e regolamentari vigenti

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole individuate dal presente Modello, i destinatari, per quanto di rispettiva competenza, sono tenuti a conoscere e a rispettare puntualmente, oltre alle norme di legge e di regolamento di volta in volta applicabili, tutta la normativa interna aziendale relativa al sistema amministrativo, finanziario e contabile

I destinatari, inoltre, sono tenuti ad operare sulla base della best practice cui l'azienda si ispira nell'esercizio delle proprie funzioni, sul fondamento che qualsiasi condotta attiva od omissiva posta in essere in violazione diretta od indiretta dei principi normativi e delle regole procedurali interne che attengono alla formazione della documentazione contabile ed alla rappresentazione esterna, così come all'esercizio delle attività di controllo e di vigilanza è da considerare come commessa in danno della azienda stessa.

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, le politiche e le procedure aziendali nonché le regole contenute nel Modello 231 e nella presente parte speciale operando, in questo modo, in coerenza con i valori e i principi che sono alla base dell'attività d'impresa in azienda

In generale, il sistema di organizzazione, gestione e controllo della società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti

Nello svolgimento delle attività sopra descritte ed , in generale, delle proprie funzioni, gli Amministratori, gli Organi Sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della Società, devono conoscere e rispettare:

- La normativa italiana e straniera applicabile alle attività svolte
- Il Codice Etico Aziendale ed Appendice Applicativa
- Il presente Modello 231
- Le procedure e le linee guida aziendali nonché tutta la documentazione attinente il sistema di organizzazione, gestione e controllo della società

3.6 - Principi e norme generali di comportamento

La presente Parte Speciale è inerente alle condotte poste in essere dai Soggetti destinatari del Modello 231 che operano, in particolare, nelle aree a Rischio Reato e nello svolgimento delle attività sensibili

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Parte Speciale, in linea generale ed al fine di perseguire la prevenzione dei Reati Societari è fatto espresso divieto a tutti i Soggetti destinatari del Modello 231 di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25-ter del D.Lgs. 231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Parte Speciale

Con riferimento a quanto espresso sopra la società obbliga i suoi Amministratori, dipendenti e soggetti terzi che agiscono in rappresentanza della società al rispetto, in particolare, dei seguenti principi:

- **I bilanci e le comunicazioni sociali previsti dalla Legge devono essere redatti con chiarezza e rappresentare in modo corretto e veritiero la situazione patrimoniale, economica e finanziaria della società**
- **È vietato, anche mediante condotte dissimulate, restituire i conferimenti effettuati dai soci o liberarli dall'obbligo di eseguirli, fuori dai casi di legittima riduzione del capitale sociale**
- **È vietato ripartire utili non effettivamente conseguiti o distribuire riserve indisponibili**
- **È vietato effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di Legge a tutela dei creditori**
- **È vietato formare od aumentare fittiziamente il capitale delle società, mediante attribuzione di quote per somma inferiore al loro valore nominale, sottoscrizione reciproca di quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti, ovvero del patrimonio delle società in caso di trasformazione.**

Quanti venissero a conoscenza di omissioni, manomissioni, falsificazioni o trascuratezza della contabilità o della documentazione di supporto sulla quale le registrazioni contabili si fondano, sono tenuti a riferire i fatti al responsabile individuato nel Legale rappresentante e all'Organismo di Vigilanza

Per ogni operazione contabile deve essere conservata agli atti sociali un'adeguata documentazione di supporto dell'attività svolta, in modo da consentire:

- **L'agevole registrazione contabile**
- **L'individuazione dei diversi livelli di responsabilità**
- **La ricostruzione accurata dell'operazione, anche al fine di ridurre la probabilità di errori interpretativi**

Le operazioni o i fatti gestionali sensibili e/o rilevanti deve essere documentati, coerenti e congrui, così che in ogni momento sia possibile identificare la responsabilità di chi ha operato (valutato, deciso, autorizzato, effettuato, rilevato nei libri, controllato l'operazione). Le responsabilità di ciascuna operazione/processo aziendale devono essere chiaramente e formalmente definite

3.7 - Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, dovranno tener conto, oltre a quanto precedentemente descritto e relativamente ad ognuna delle fattispecie di reato ritenute rilevanti per la Società, delle previsioni di seguito Indicate.

False comunicazioni sociali (art. 2621 c.c.)
False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.)

Ai fini di prevenire i reati di false comunicazioni sociali e di false comunicazioni sociali in danno della Società, dei soci o dei creditori, i soggetti sopra indicati hanno l'espresso obbligo di tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi una informazione veritiera e

corretta sulla situazione economica, patrimoniale e finanziaria della società

A tale riguardo, deve essere loro cura, a titolo esemplificativo, astenersi da:

a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società
b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società
c) porre la massima attenzione e accuratezza nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni utilizzati in modo tale da fornire una presentazione veritiera e corretta corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della società e sull'evoluzione della sua attività

Inoltre, gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, dovranno tener conto, oltre a quanto precedentemente definito delle procedure e regole aziendali che prevedono:

- Il rispetto del Codice Etico e delle sue specifiche previsioni riguardanti il corretto comportamento di tutti i soggetti coinvolti nelle attività di formazione del bilancio o di altri documenti similari, quali ad esempio:
    a) Massima collaborazione, veridicità, autenticità ed originalità della documentazione e delle informazioni trattate
    b) Chiarezza e correttezza della rappresentazione patrimoniale e finanziaria della società
    c) Completezza, segnalazione di eventuali omissioni, manomissioni, falsificazioni o trascuratezza della contabilità o della documentazione di supporto sulla quale le registrazioni contabili si fondano, etc.,
- Il rispetto del calendario di chiusura, finalizzato alla redazione del bilancio indicante:
    a) Data di chiusura dei periodi contabili
    b) Data di chiusura delle scritture contabili
    c) Data di predisposizione della Bozza del Bilancio e del Bilancio Definitivo
- La chiara definizione della responsabilità della veridicità, autenticità ed originalità della documentazione e delle informazioni e dei dati forniti dal Responsabile della determinazione delle varie poste/fondi
- Il supporto documentale a corredo delle informazioni e dei dati forniti dal Responsabile di cui al punto precedente
- Il controllo, da parte del consulente esterno incaricato nella predisposizione del bilancio delle voci aggregate di Bilancio confrontandole con quelle dell'anno precedente, mantenendo evidenza del riscontro effettuato e delle eventuali motivazioni relative a scostamenti anomali
- La tracciabilità informatica delle operazioni effettuate
- La tracciabilità dell'invio della bozza del Bilancio, alcuni giorni precedenti l'approvazione da parte dell'Amministratore Unico per permettere allo stesso la verifica delle connotazioni essenziali del bilancio prima che sia sottoposto all'Assemblea per l'approvazione

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Societari aziendali (e dei Dipendenti e Collaboratori esterni nella misura necessaria alle funzioni dagli stessi svolte) di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o

indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-ter del D.Lgs. n. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale

La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società
2. tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure interne, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei dati e delle informazioni relative agli strumenti finanziari emessi da altre società del Gruppo, necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della società, sull'evoluzione della sua attività, nonché sugli strumenti finanziari e relativi diritti
3. osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere
4. assicurare il regolare funzionamento degli Organi Societari, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare
5. evitare di porre in essere operazioni simulate o diffondere notizie false idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari
6. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate

Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:

- con riferimento al precedente punto 1:
  - rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà sulla situazione economica, patrimoniale e finanziaria della società
  - omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società

- con riferimento al precedente punto 2:
  - alterare i dati e le informazioni destinati alla predisposizione dei prospetti informativi eventualmente predisposti dalla società
  - illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della società e sull'evoluzione della sua attività, nonché sugli strumenti finanziari e relativi diritti

- con riferimento al precedente punto 3:
  - restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale
  - ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva
  - acquistare o sottoscrivere azioni della società o di società controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale
  - effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno
  - procedere a formazione e/o aumenti fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale

- con riferimento al precedente punto 4:
  - porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione della gestione sociale da parte del collegio sindacale o della società di revisione o che comunque la ostacolino
  - determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare

- con riferimento al precedente punto 5:
  - pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio aventi ad oggetto strumenti finanziari non quotati ed idonei ad alterarne sensibilmente il prezzo ovvero al fine di incidere sul pubblico affidamento in merito alla stabilità patrimoniale societaria

- con riferimento al precedente punto 6:
  - omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di vigilanza cui è soggetta l'attività aziendale, nonché omettere di dar corso con sollecitudine all'invio dei dati e della documentazione eventualmente richiesta dalle predette autorità
  - esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società
  - porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte dell'Autorità di vigilanza.

Ai fini dell'attuazione delle regole elencate al precedente capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali specifici qui di seguito descritti.
Predisposizione delle comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della società

I documenti contenenti comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della società devono essere redatti in base alle specifiche procedure aziendali in essere che:

- determinano con chiarezza e completezza i dati e le notizie che ciascuna funzione deve fornire ed i controlli che devono essere svolti su detti dati e notizie, nonché i criteri contabili per l'elaborazione dei dati e la tempistica per la loro consegna alle funzioni responsabili
- prevedono la trasmissione di dati ed informazioni alla funzione responsabile attraverso un sistema che consente la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema

In particolare, nei processi contabili e più in generale di produzione di documenti che rappresentano situazioni economiche, finanziarie e patrimoniali della società le funzioni aziendali coinvolte sono tenute al rispetto dei seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione
- separazione dei compiti e delle funzioni
- documentazione delle decisioni e dei controlli
- accurata gestione delle notizie riservate

Predisposizione dei prospetti informativi

La redazione, o partecipazione alla redazione, di prospetti informativi dovrà essere effettuata sulla base di procedure che si fondano sui seguenti principi:

- utilizzo di procedure coerenti con quelle adottate per la predisposizione delle comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della società
- ove esistenti, utilizzo di informazioni contenute in comunicazioni già pubblicate
- utilizzo di informazioni previsionali condivise dalle funzioni coinvolte ed approvate dall'Amministratore Unico

Gestione dei rapporti con la società di revisione contabile in ordine all'attività di comunicazione da parte di quest'ultima a terzi relativa alla situazione economica, patrimoniale e finanziaria della società

Nei rapporti tra l'azienda e la società di revisione contabile sono adottati i seguenti presidi:

- Gli incarichi di consulenza, aventi ad oggetto attività diversa dalla revisione contabile, vengono conferiti alla società di revisione su proposta del Collegio Sindacale
- È vietato il conferimento a soggetti che siano parte della rete o del network cui appartiene la società di revisione di incarichi diversi dalla revisione contabile che appaiono incompatibili con quest'ultima, in quanto suscettibili di pregiudicare l'indipendenza della società di revisione incaricata
- L'assemblea dei soci viene informata dell'eventuale conferimento di ulteriori incarichi rispetto a quello di revisione contabile alla società di revisione incaricata nonché dell'eventuale conferimento di incarichi a soggetti che siano parte della rete o del network a cui appartiene la società di revisione.

Operazioni relative al capitale sociale

Tutte le operazioni sul capitale sociale nonché la costituzione di società, l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate nel rispetto delle regole di corporate governance e delle procedure aziendali e di gruppo all'uopo predisposte

Predisposizione delle comunicazioni alle Autorità di vigilanza e gestione dei rapporti con le stesse

Con riferimento alle attività societarie soggette alla vigilanza di pubbliche autorità, in base alle specifiche normative applicabili, al fine di prevenire la commissione dei reati di false comunicazioni alle autorità e di ostacolo alle funzioni di vigilanza, le attività soggette a vigilanza devono essere svolte in base a procedure aziendali contenenti la disciplina delle modalità e l'attribuzione di specifiche responsabilità in relazione:

- alle segnalazioni periodiche alle autorità previste da leggi e regolamenti
- alla trasmissione a queste ultime dei documenti previsti in leggi e regolamenti
- alla trasmissione di dati e documenti specificamente richiesti dalle Autorità di vigilanza
- al comportamento da tenere nel corso degli accertamenti ispettivi

I principi posti a fondamento di tali procedure sono:

- attuazione di tutti gli interventi di natura organizzativo-contabile necessari ad estrarre i dati e le informazioni per la corretta compilazione delle segnalazioni ed il loro puntuale invio all'Autorità di vigilanza, secondo le modalità ed i tempi stabiliti dalla normativa applicabile
- adeguata formalizzazione delle procedure in oggetto e successiva documentazione dell'esecuzione degli adempimenti in esse previsti, con particolare riferimento all'attività di elaborazione dei dati
- nel corso dell'attività ispettiva, deve essere prestata da parte delle funzioni e delle articolazioni organizzative ispezionate la massima collaborazione all'espletamento degli accertamenti e non devono essere tenute condotte tali che siano di ostacolo all'esercizio delle funzioni di vigilanza (ad es. espressa opposizione, rifiuti ingiustificati, ritardi nella trasmissione o nella consegna di documenti). In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati ritengano necessario acquisire, previo il consenso del responsabile incaricato di interloquire con l'autorità
- alle ispezioni devono partecipare i soggetti a ciò espressamente delegati. L'Organismo di Vigilanza dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura della Direzione aziendale di volta in volta interessata. Di tutto il procedimento relativo all'ispezione devono essere redatti gli appositi verbali, che verranno conservati dall'Organismo di Vigilanza.

Altre regole finalizzate alla prevenzione dei reati societari in genere

A fianco delle regole e delle procedure esistenti, si dispone l'attuazione dei seguenti presidi integrativi:

- **previsione di riunioni tra Collegio Sindacale e Organismo di Vigilanza per verificare l'osservanza della disciplina**

in tema di normativa societaria e di corporate governance

- **trasmissione al Collegio Sindacale, con congruo anticipo, di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o sui quali esso debba esprimere un parere ai sensi di legge**
- **partecipazione dell'Organismo di Vigilanza alle riunioni assembleari mediante apposito invito predisposto dalla funzione Segreteria. L'Organismo di Vigilanza valuterà l'utilità della propria partecipazione**
- **formalizzazione e/o aggiornamento di regolamenti interni e procedure aventi ad oggetto l'osservanza della normativa societaria**

3.8 - I controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della società

L'Organismo di Vigilanza dovrà avere evidenza e mantenere traccia:

- di quanto posto in essere nella società al fine di fornire indicazioni per la corretta redazione del bilancio
- per quanto concerne il conferimento dell'incarico, l'Organismo di Vigilanza dovrà mantenere agli atti evidenza delle valutazioni circa le proposte, gli ambiti e le scelte effettuate da sottoporre all' Amministratore Unico degli incarichi conferiti.

L'Organismo di Vigilanza dovrà, inoltre, esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni

Inoltre, i compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati societari sono i seguenti:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale
- monitorare sul rispetto delle procedure interne per la prevenzione dei reati societari. L'Organismo di Vigilanza è tenuto alla conservazione delle evidenze dei controlli e delle verifiche eseguiti
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante

☑ **Sistema di gestione**
- ☑ *Modello di organizzazione*
- ☐ *Codice etico*
- ☐ *Analisi dei rischi*

☐ **Procedure**

☐ **Modulistica**

Digitronica.IT
Your Security Our Software

PARTE SPECIALE – SEZ. C – REATI DI OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO
(*Art. 25-septies del D.Lgs. 231/01*)

MOGC-SPE-03

Organizzazione

Digitronica.IT S.p.A.

Sede: Viale del Lavoro, 52 Verona
Phone: 045 50 19 01
Fax: 045 50 22 58
Email: info@digitronica.it
Pec: digitronica.it@pec.it

MOGC 231 – PARTE SPECIALE

ai sensi del D.Lgs. n. **231** del 8 Giugno 2001 e s.m.i.

Master	☐
Copia controllata	☐
Copia non controllata	☐
Numero della copia	☐

Emissione DG	Data		Firma	
Approvazione DG	Data		Firma	
Approvazione ODV	Data		Firma	

Stato delle revisioni

Versione	Data	Descrizione	Autore
00	*04/06/2019*	Prima emissione	Digitronica.IT Srl
01	*01/12/2020*	Aggiornamento	Digitronica.IT S.p.A.
02	*01/04/2022*	Aggiornamento	Digitronica.IT S.p.A.
03	*22/01/2024*	Aggiornamento OdV	Digitronica.IT SpA

PARTE SPECIALE – SEZ. C – REATI DI OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

(*Art. 25-septies del D.Lgs. 231/01*)

MOGC-SPE-03

Indice generale della sezione

Modello di Organizzazione, Gestione e Controllo – Parte speciale

4.1 - Introduzione e funzione del reato di omicidio colposo e lesioni colpose commesse con violazione delle norme antinfortunistiche

Termini relativi alle norme per la salvaguardia della salute e sicurezza sul lavoro

ASPP o Addetti al Servizio di Prevenzione e Protezione
I soggetti in possesso delle capacità e dei requisiti professionali di cui all'art. 32 del Decreto Sicurezza designati per l'espletamento dei compiti rientranti nel Servizio di Prevenzione e Protezione

Cantiere Temporaneo o Mobile o Cantiere
Qualunque luogo in cui si effettuano lavori edili o di ingegneria civile così come individuati nell'allegato X del Decreto Sicurezza, ovvero, lavori di costruzione, manutenzione, riparazione, demolizione, conservazione, risanamento, ristrutturazione, equipaggiamento, trasformazione, rinnovamento o smantellamento di opere fisse, permanenti o temporanee, comprese le linee elettriche e le parti strutturali degli impianti elettrici. Sono, inoltre, lavori di costruzione edile o di ingegneria civile gli scavi ed il montaggio e lo smontaggio di elementi prefabbricati utilizzati per i lavori edili o di ingegneria civile

Committente
Il soggetto per conto del quale viene realizzata l'intera opera edile o di ingegneria civile, indipendentemente da eventuali frazionamenti della sua realizzazione secondo quanto disposto dagli artt. 88 e ss. del Decreto Sicurezza.

Coordinatore per l'Esecuzione dei Lavori
Il soggetto incaricato dal committente o dal responsabile dei lavori tra l'altro, di verificare, con opportune azioni di coordinamento e controllo, l'applicazione, da parte delle imprese esecutrici e dei lavoratori, anche autonomi, delle disposizioni loro pertinenti contenute nel piano di sicurezza e coordinamento e di verificare altresì l'idoneità del piano operativo di sicurezza, assicurandone la coerenza con il primo.

Coordinatore per la Progettazione
Il soggetto, incaricato dal committente o dal responsabile dei Lavori, di redigere il piano di sicurezza e di coordinamento e di predisporre un fascicolo contenente le informazioni utili ai fini della prevenzione e della protezione dai rischi cui sono esposti i lavoratori.

Datore di Lavoro
Il soggetto titolare del rapporto di lavoro o, comunque, il soggetto che, secondo il tipo e l'organizzazione dell'impresa, ha la responsabilità dell'impresa stessa ovvero dell'unità produttiva in quanto titolare dei poteri decisionali e di spesa. È responsabile di provvedere all'attuazione di tutti gli obblighi fissati dal D.Lgs. 81/08 s.m.i. Gli obblighi non delegabili sono i seguenti:

- *La valutazione di tutti i rischi e la conseguente elaborazione del documento (Art. 28 Del D.Lgs. 81/08)*

- *La designazione del responsabile del servizio di prevenzione e protezione dei rischi*

Decreto Sicurezza
Il Decreto Legislativo 9 Aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e sicurezza nei luoghi di lavoro"

Dirigente
Il soggetto che, in ragione delle competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando sulla stessa

DUVRI o Documento Unico di Valutazione dei Rischi per le Interferenze
Il documento redatto dal datore di lavoro committente contenente una valutazione dei rischi che indichi le misure per eliminare o, ove ciò non risulti possibile, ridurre al minimo i rischi da interferenze nei contratti di appalto, d'opera o di somministrazione ai sensi dell'art. 26 del Decreto Sicurezza

DVR o Documento di Valutazione dei Rischi
Il documento redatto dal datore di lavoro contenente una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro ed i criteri per la suddetta valutazione, l'indicazione delle misure di prevenzione e protezione e dei dispositivi di protezione individuale conseguente a tale valutazione, il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, l'indicazione del nominativo del RSPP, del RLS e del medico competente che abbia partecipato alla valutazione del rischio, nonché l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione

Fascicolo dell'Opera
Il fascicolo predisposto a cura del coordinatore per la progettazione, eventualmente modificato nella fase esecutiva in funzione dell'evoluzione dei lavori ed aggiornato a cura del committente a seguito delle modifiche intervenute in un'opera nel corso della sua esistenza, contenente le informazioni utili ai fini della prevenzione e della protezione dei rischi cui sono esposti i lavoratori

Lavoratori
Soggetti che svolgono un'attività lavorativa nell'ambito della struttura organizzativa della società e contribuiscono, insieme al datore di lavoro, ai dirigenti ed ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro

Medico Competente
Il medico preposto all'attività di sorveglianza sanitaria. Il medico deve inoltre possedere uno dei titoli e dei requisiti formali e professionali indicati nel decreto sicurezza che collabora con il datore di lavoro, secondo quanto previsto all'Art.29 del D.Lgs.81/08 e s.m.i, ai fini della valutazione dei rischi e al fine di effettuare la sorveglianza sanitaria (di cui all'Art. 41 del D.Lgs 81/08 e s.m.i.) ed adempiere tutti gli altri compiti di cui al decreto sicurezza

Preposto

PARTE SPECIALE – SEZ. C – REATI DI OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

(*Art. 25-septies del D.Lgs. 231/01*)

MOGC-SPE-03

Il soggetto che in ragione delle competenze professionali e nei limiti dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende all'attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa

Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro

I reati di cui all'Art. 25-septies del D.Lgs. 231/2001, ovvero l'omicidio colposo (Art. 589 c.p.) e le lesioni personali colpose gravi o gravissime (Art. 590 terzo comma c.p.) commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro

RLS o Rappresentante dei Lavoratori per la Sicurezza

Soggetto eletto o designato per rappresentare i lavoratori in relazione agli aspetti della salute e sicurezza sul lavoro

RSPP o Responsabile del Servizio di Prevenzione e Protezione

Il soggetto responsabile del servizio di prevenzione e protezione nominato dal datore di lavoro a cui risponde secondo quanto previsto dall'Art. 33 del D.Lgs. 81/08 e s.m.i.

Responsabile dei Lavori

Il soggetto che può essere incaricato dal committente ai fini della progettazione, dell'esecuzione o del controllo dell'esecuzione dell'opera o di una parte della procedura

Sorveglianza Sanitaria

L'insieme degli atti medici finalizzati alla tutela dello stato di salute e sicurezza dei lavoratori in relazione all'ambiente di lavoro, ai fattori di rischio professionali, ed alle modalità di svolgimento dell'attività lavorativa

SPP o Servizio di Prevenzione e Protezione

L'insieme delle persone, sistemi e mezzi esterni o interni alla società finalizzati all'attività di prevenzione e protezione dei rischi professionali

SLL

Salute e sicurezza dei lavoratori

Addetto al Primo Soccorso e addetto alla prevenzione incendi

Soggetti incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza

Referente Tecnico

Soggetto incaricato di assicurare la corretta realizzazione, in conformità alle norme e specifiche tecniche di progetto o del capitolato speciale, delle opere e dei servizi commissionati ad appaltatori/fornitori

4.2 - Criteri per la definizione del reato di omicidio colposo e lesioni colpose commesse con violazione delle norme antinfortunistiche

I reati contro la persona sono ipotesi aggravate dei delitti di omicidio colposo e lesioni personali colpose

Tale aggravante consiste nella violazione delle norme per la prevenzione degli infortuni sul lavoro, sussiste non soltanto quando sia contestata la violazione di specifiche norme per la prevenzione degli infortuni sul lavoro, ma anche quando la contestazione ha per oggetto l'omissione dell'adozione di misure e/o accorgimenti per la più efficace tutela dell'integrità fisica dei lavoratori e, più in generale, la violazione di tutte le norme che, direttamente o indirettamente, tendono a garantire la sicurezza del lavoro in relazione all'ambiente in cui deve svolgersi.

4.3 - Le fattispecie di reato richiamate dal D.Lgs. 231/01

Si provvede qui di seguito a fornire una breve descrizione dei reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro indicati all'Art. 25-septies del Decreto

Tale articolo, originariamente introdotto dalla Legge 3 Agosto 2007 n. 123, e successivamente sostituito ai sensi dell'art. 300 del Decreto Sicurezza, prevede l'applicazione di sanzioni pecuniarie ed interdittive agli Enti i cui esponenti commettano i reati di cui agli art. 589 (omicidio colposo) e 590 terzo comma (lesioni personali colpose gravi o gravissime) del codice penale, in violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Le fattispecie delittuose inserite all'art. 25-septies riguardano unicamente le ipotesi in cui l'evento sia stato determinato non già da colpa di tipo generico (e dunque per imperizia, imprudenza o negligenza) bensì da "colpa specifica" che richiede che l'evento si verifichi a causa della inosservanza delle norme per la prevenzione degli infortuni sul lavoro

Il Consiglio dei Ministri in data 1 Aprile 2008 ha approvato il D.Lgs. 81/08 attuativo della delega di cui all'Art. 1 della L. 3 Agosto 2007 n. 123 in materia della salute e sicurezza nei luoghi di lavoro modificato dal D.Lgs. 3 Agosto 2009 n. 106 "Disposizioni integrative e correttive del D.Lgs 81/08"

4.3.1 - Omicidio Colposo (Art. 589 c.p.)

Tale ipotesi di reato si configura nei confronti di "Chiunque cagiona per colpa la morte di una persona"

I soggetti che possono rispondere del reato sono tutti i soggetti tenuti ad osservare o far osservare le norme di prevenzione o protezione, vale a dire i datori di lavoro, i dirigenti, i preposti, i soggetti destinatari delle deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro nonché i medesimi lavoratori

La colpa, nel caso che ci interessa, consiste nell'avere il soggetto agito in violazione delle norme sulla prevenzione degli infortuni sul lavoro o meglio nella mancata adozione delle misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili alla luce dell'esperienza e delle più avanzate conoscenze tecnico scientifiche

Se il reato in oggetto è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro, la pena è della reclusione da due a sette anni

Le misure di sicurezza vanno intese sia in senso statico vale a dire quale obbligo di adottare le misure di protezione e sicurezza oggettiva, sia in senso dinamico da intendersi come obbligo di formare ed informare i lavoratori circa i rischi propri dell'attività lavorativa nonché sulle misure idonee per evitare i rischi o ridurli al minimo

La colpa per violazione delle norme per la prevenzione degli infortuni sul lavoro, pertanto, può essere ravvisata non solo in caso di violazione delle specifiche norme per la prevenzione degli infortuni sul lavoro ma anche nel caso in cui l'evento (che in caso di omicidio consiste nella morte) dipenda dall'omessa adozione di quelle misure ed accorgimenti imposti all'imprenditore ai fini della tutela dell'integrità fisica e della personalità del lavoratore da differenziare a seconda della tipologia di lavoro e tenendo conto della tecnica e dell'esperienza (art. 2087 del codice civile)

L'ente risponde, ai sensi del D.Lgs. 231/2001, qualora abbia tratto un vantaggio dall'evento dannoso che può consistere, ad esempio, in un risparmio di costi o di tempi per non aver adottato le misure di prevenzione degli infortuni sul lavoro

Il datore di lavoro risponde, ad esempio, di omicidio colposo nel caso in cui la morte sia derivata dall'inosservanza delle norme sulla prevenzione degli infortuni sul lavoro qualora l'evento della morte si sia verificato nei confronti di un dipendente oppure di un soggetto estraneo all'ambiente di lavoro purché la presenza sul luogo di lavoro non sia eccezionale o atipica

4.3.2 - Lesioni personali colpose gravi e gravissime (Art. 590, comma 3 c.p.)

Tale ipotesi di reato si configura nei confronti di "Chiunque cagiona per colpa una lesione personale"

La colpa richiesta dall'art. 25-septies del D.Lgs. 231/2001, consiste nella violazione delle norme per la prevenzione degli infortuni sul lavoro e di igiene e sicurezza. L'ente, risponde ai sensi del D.Lgs. 231/2001 sia per le ipotesi di lesioni gravi che per i casi di lesioni gravissime qualora abbia tratto un vantaggio concreto da intendersi, ad esempio, come già si è detto, quale una riduzione dei costi per approntare le misure di sicurezza richieste dalla normativa vigente o, comunque, dovute in considerazione delle nuove acquisizioni tecnologiche

Il delitto, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relativi all'igiene del lavoro o che abbiamo determinato una malattia professionale, è perseguibile d'ufficio

Se il reato è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro, la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da 500 Euro a 2.000 Euro e la pena per le lesioni gravissime è della reclusione da uno a tre anni

Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo, ma la pena della reclusione non può superare gli anni cinque

Ai sensi del comma 1 dell'art. 583 cod. penale, la lesione è considerata **grave** nei seguenti casi:

1. Se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni
2. Se il fatto produce l'indebolimento permanente di un senso o di un organo

Ai sensi del comma 2 dell'art. 583 cod. penale, la lesione è considerata invece **gravissima** se dal fatto deriva:

1. Una malattia certamente o probabilmente insanabile
2. La perdita di un senso
3. La perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella
4. La deformazione, ovvero lo sfregio permanente del viso

Esclusione della responsabilità amministrativa della società

Come già indicato nella Parte Generale del Modello, il D.Lgs. n. 81/2008, all'art. 30, ha indicato le caratteristiche e i requisiti che deve un modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al Decreto.

Pertanto nella predisposizione del Modello e nella definizione degli standard di controllo la società ha tenuto conto:

- Delle previsioni del Decreto
- Della vigente disciplina legislativa della prevenzione dei rischi lavorativi
- Del British Standard OHSAS 18001:2007
- Delle Linee Guida Confindustria
- Dell'art. 30 del D.Lgs. 81/2008

4.4 - Le sanzioni previste dal Decreto (art.55 D.Lgs 81/08)

Per entrambe le fattispecie delittuose sopra indicate - ossia omicidio colposo e lesioni personali colpose gravi o gravissime - gli enti sono soggetti ad una sanzione pecuniaria fino a 1000 quote (si consideri a tal riguardo che il valore di ogni quota può essere determinato, sulla base delle condizioni economiche e patrimoniali dell'ente, tra un minimo di 258 e un massimo di 1549 euro)

Perché si venga a configurare la responsabilità amministrativa della società ai sensi del Decreto Legislativo 8 giugno 2001, n. 231, l'art. 5 del Decreto medesimo esige però che i reati siano stati commessi nel suo interesse o a suo vantaggio (ad esempio in termini di risparmi di costi per la salute e sicurezza sul lavoro) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità' organizzativa dotata di autonomia finanziaria e funzionale nonchè da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso

L'ente non risponde se le persone hanno agito nell'interesse esclusivo proprio o di terzi.

Nel caso di condanna per uno dei reati sopra indicati, la società potrebbe essere assoggettata anche ad una sanzione interdittiva per una durata non inferiore a tre mesi e non superiore ad un anno

Tali sanzioni interdittive possono consistere in:

- 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 ed eventuale revoca di quelli già concessi
- Divieto di pubblicizzare beni o servizi

4.5 - Le attività sensibili relative ai reati di omicidio colposo e lesioni colpose commesse

Le principali aree aziendali a potenziale rischio reato relativamente alle fattispecie di cui all'art.25-septies del D.Lgs. 231/01 sono identificate e valutate nell'ambito dei documenti aziendali di valutazione dei rischi, predisposti ai sensi della normativa di riferimento e costantemente aggiornati in relazione all'evoluzione delle caratteristiche dell'attività produttiva

Tuttavia, come precisato dalle Linee Guida di Confindustria per la costruzione dei Modelli di organizzazione, gestione e controllo ex D.Lgs. 231/01, non è possibile individuare e limitare a priori alcun ambito di attività, dal momento che tale casistica di reati può, di fatto, investire la totalità delle componenti aziendali

In altri termini i oggetto della presente Parte Speciale potrebbero astrattamente essere commessi in tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro

Poiché la valutazione dei rischi rappresenta l'adempimento cardine per la garanzia della salute e della sicurezza dei lavoratori e poiché costituisce il principale strumento per procedere all'individuazione delle misure di tutela, siano esse la riduzione o l'eliminazione del rischio, l'operazione di individuazione e di rilevazione dei rischi deve essere effettuata con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza

Il Modello, pertanto, prevede un costante aggiornamento del Documento di Valutazione dei Rischi (DVR), fornendo così evidenza del suo continuo adeguamento e della sua completezza

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nel Modello e nella parte speciale del presente Modello

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree di operatività ritenute più specificamente a rischio per la società risultano essere, ai fini della presente Parte Speciale del Modello, le seguenti:

- Attività di ufficio svolta dal personale dipendente, in particolare per ciò che concerne l'utilizzo di videoterminali
- Attività svolta da personale esterno presso la sede della società, quali fornitori di servizi in base a contratti di appalto, d'opera o di somministrazione (di cui all'art. 26 del Decreto Sicurezza).

PARTE SPECIALE – SEZ. C – REATI DI OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

(*Art. 25-septies del D.Lgs. 231/01*)

MOGC-SPE-03

Nell'ambito delle suddette aree di operatività, in virtù della probabilità che in tali contesti l'inosservanza delle norme poste a tutela della salute e sicurezza sul lavoro possa determinare uno degli eventi dannosi di cui all'art. 25 septies, sono state individuate le seguenti attività sensibili:

- Determinazione delle procedure interne in tema di salute e sicurezza sul lavoro volte a definire i compiti e le responsabilità in materia di sicurezza e a garantire una corretta gestione di tutti gli adempimenti posti in capo a ciascun destinatario così come disposti dal Decreto Sicurezza e dalla normativa primaria e secondaria ad esso collegata
- Attribuzione di responsabilità in materia di salute e sicurezza sul lavoro, con particolare riferimento a:
    - Attribuzioni di compiti e doveri in capo a ciascun Destinatario
    - Attività del Servizio Prevenzione e Protezione e del Medico Competente
- Individuazione dei pericoli all'interno della sede dell'azienda e valutazione dei rischi, con particolare riferimento a:
    - Stesura del Documento di Valutazione dei Rischi (DVR)
    - Valutazione dei rischi delle interferenze
    - Gestione dei contratti di appalti
- Sensibilizzazione di tutti i soggetti che, a diversi livelli, operano nell'ambito della struttura aziendale attraverso un'adeguata attività di informazione e la programmazione di piani di formazione in tema di salute e sicurezza nei luoghi di lavoro
- Attuazione di adeguate attività di monitoraggio, verifica ed ispezione, in particolare per ciò che concerne:
    - L'aggiornamento delle misure in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fine della salute e sicurezza sul lavoro
    - La gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme, attraverso l'eventuale irrogazione di provvedimenti disciplinari

4 .6 - Organi e funzioni aziendali coinvolte

In relazione alle descritte attività sensibili, si ritengono particolarmente coinvolti alcuni organi e funzioni aziendali

Amministrazione

In relazione all'attività di gestione dei Dipendenti relativamente ad eventuali provvedimenti disciplinari ed agli adempimenti infortunistici

Per attività di informazione e la programmazione di piani di formazione in tema di salute e sicurezza nei luoghi di lavoro

Amministratore Unico

Con riferimento all'approvazione del budget annuale di spesa in particolare per ciò che concerne i costi per la sicurezza. In qualità di Datore di Lavoro della società secondo la definizione di cui al Decreto Sicurezza, in relazione all'adempimento di tutti i compiti non delegabili a lui attribuiti dal suddetto decreto (e dunque, a titolo esemplificativo, attività di valutazione dei rischi e predisposizione del relativo Documento di Valutazione dei Rischi o valutazione dei rischi delle interferenze), nonché in merito all'inibizione dei comportamenti posti in violazione delle norme a tutela della salute e sicurezza dei Lavoratori attraverso l'adozione di eventuali provvedimenti disciplinari

Lavoratori

In particolare con riferimento ai soggetti incaricati dell'attuazione delle misure di prevenzione incendi, di evacuazione dei luoghi di lavoro in caso di pericolo, di salvataggio, di primo soccorso e di gestione delle emergenze e, in generale, con riferimento a tutti, in merito all'osservanza delle norme poste a tutela dell'incolumità propria e altrui

4.7 - Principi e norme generali di comportamento

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Soggetti Apicali o in Posizione Apicale, dipendenti, collaboratori, fornitori della società nonché, nella misura in cui non rientrino in queste definizioni, dalle figure rilevanti di cui al successivo paragrafo (destinatari)

Obiettivo della presente Parte Speciale è che tutti i destinatari si attengano – in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti della società – a regole di condotta conformi a quanto prescritto nella medesima Parte Speciale al fine di prevenire e impedire il verificarsi dei Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei Lavoratori, così come individuati dal Decreto Sicurezza, si prevede che la gestione della tutela della salute e sicurezza sul lavoro (SSL) costituisce parte integrante della gestione aziendale

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nel Modello e nella presente parte speciale del Modello

In generale, il sistema di organizzazione, gestione e controllo della Società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività e in generale, delle proprie funzioni, gli amministratori, gli organi sociali, i lavoratori, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, devono conoscere e rispettare:

- Leggi e regolamenti in tema di salute e sicurezza negli ambienti di lavoro
- Il Codice Etico
- Il presente Modello
- Le procedure/linee guida aziendali, la documentazione e le disposizioni inerenti la struttura organizzativa

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

- Conoscibilità all'interno della società
- Delimitazione dei ruoli, con una descrizione dei compiti di ciascuna funzione e dei relativi poteri
- Descrizione delle linee di riporto

Nello specifico, la società, è dotata di una struttura organizzativa in conformità a quella prevista dalla normativa prevenzionistica vigente.

In coerenza con lo schema organizzativo e funzionale dell'azienda sono stati definiti i compiti e le responsabilità in materia di SSL a partire dal Datore di Lavoro fino al lavoratore

La società, come previsto dal D.Lgs.81/08 e s.m.i, deve garantire il rispetto delle normative in tema di tutela della SSL, di tutela dell'ambiente nonché assicurare in generale un ambiente di lavoro sicuro, sano e idoneo allo svolgimento dell'attività, anche attraverso:

- Una continua analisi del rischio e della criticità dei processi e delle risorse da proteggere
- La programmazione della prevenzione, mirando ad un complesso che integri in modo coerente nella prevenzione e condizioni lavorative e organizzative dell'azienda nonché l'influenza dei fattori dell'ambiente di lavoro
- Il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro
- L'eliminazione/riduzione al minimo dei rischi in relazione alle conoscenze acquisite in base al progresso tecnico, privilegiando gli interventi alla fonte
- La sostituzione di ciò che è pericoloso con ciò che non è pericoloso o che è meno pericoloso
- Il controllo e l'aggiornamento delle metodologie di lavoro
- Il controllo sanitario dei lavoratori, con particolare riguardo ai rischi specifici
- Attività di informazione, formazione, consultazione e partecipazione dei lavoratori ovvero dei loro rappresentanti, dei dirigenti e dei preposti sulle questioni riguardanti la sicurezza e la salute sul luogo di lavoro
- La partecipazione e consultazione dei lavoratori e dei loro rappresentanti
- La programmazione delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione del Codice Etico e di buone prassi
- La formalizzazione di istruzioni adeguate ai lavoratori
- L'uso di segnali di avvertimento e sicurezza
- La regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti
- La definizione di adeguate misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato

Le misure relative alla SSL non devono in nessun caso comportare oneri finanziari per i lavoratori

Nella scelta dei fornitori di beni o servizi, ivi inclusi in materia di SSL, devono essere privilegiati l'affidabilità del fornitore e la sua capacità di assolvere correttamente alle obbligazioni assunte, oltre al rapporto qualità/prezzo del bene o della prestazione offerta.

È fatto espresso divieto di:

- Modificare o disattivare, senza autorizzazione i dispositivi di protezione individuali o collettivi
- Modificare o togliere, senza autorizzazione, i dispositivi di sicurezza o di segnalazione o di controllo
- Fabbricare, acquistare, noleggiare e utilizzare impianti, macchine, attrezzature o altri mezzi tecnici, inclusi dispositivi di protezione individuali e collettivi, non adeguati o non rispondenti alle disposizioni vigenti in materia di sicurezza
- Accedere ad aree di lavoro a cui non si è autorizzati
- Svolgere di propria iniziativa operazioni che non siano di competenza o che possano compromettere la sicurezza propria o di altri lavoratori

4.8 - Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, etc.,) gli amministratori, gli organi sociali, i lavoratori, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, nello svolgimento delle attività sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'art. 25 septies, al rispetto della normativa vigente, delle regole e procedure aziendali emesse a regolamentazione delle attività a rischio

Tali regole e procedure sono contenute in una struttura documentale articolata in:

- Istruzioni di lavoro
- Registrazioni relative agli aspetti inerenti la SSL tra le quali i registri di dati specifici
- La formazione, i risultati dei monitoraggi ed i risultati dei riesami
- Altri documenti (legislazione, norme tecniche, etc.,)

La Società, nella predisposizione delle procedure in materia di SSL, rivolge particolare attenzione all'esigenza di garantire il rispetto dei seguenti principi:

- Devono essere formalmente identificate e documentate le responsabilità in materia di SSL, attraverso disposizioni organizzative e deleghe specifiche rilasciate da parte dei soggetti competenti e comunicate ai terzi interessati.
- Deve essere nominato il Medico Competente, devono, altresì, essere definiti appositi ed adeguati flussi informativi verso il Medico Competente in relazione ai processi ed ai rischi connessi all'attività produttiva.
- Devono essere tempestivamente identificati e valutati dal Datore di Lavoro i rischi per la SSL ivi compresi quelli riguardanti i lavoratori esposti a rischi particolari, deve, inoltre, essere tenuta in adeguata considerazione la struttura aziendale, la natura dell'attività, l'ubicazione dei locali e delle aree di lavoro, l'organizzazione del personale, i macchinari, le attrezzature e gli impianti impiegati nelle attività e nei relativi cicli di protezione. La valutazione dei rischi deve essere documentata attraverso l'elaborazione, ai sensi della normativa prevenzionistica vigente, di un DVR che contenga quanto prescritto all'Art. 28 del D.Lgs. 81/08 e succ. mod.

- Il DVR deve essere elaborato dal DDL in collaborazione con il RSPP e il medico competente. Il DVR deve essere custodito presso il sito di riferimento ed aggiornato periodicamente e comunque in occasione di modifiche dell'organizzazione del lavoro significative ai fini della salute e sicurezza dei lavoratori, o in relazione al grado di evoluzione della tecnica, della prevenzione o della protezione o a seguito di infortuni significativi o quando i risultati della sorveglianza sanitaria ne evidenzino la necessità. A seguito di tale rielaborazione, le misure di prevenzione debbono essere aggiornate
- La valutazione del rischio deve essere condotta sviluppando il criterio di analisi dei rischi per singola fonte, identificata dalle norme di legge o ragionevolmente prevedibile, individuando nel documento di metodica le modalità di esecuzione. Il documento di metodica è quindi il punto di riferimento per la rappresentazione della metodologica di tutti i rischi, a cui fanno riferimento:

    - Le schede di valutazione del rischio specifica per mansione, sulla base del processo lavorativo e dell'organizzazione presente, atte ad evidenziare i rischi presenti per singole fasi o gruppi di fasi lavorative, e le misure tecniche, organizzative e formative messe in atto per la loro prevenzione
    - Le relazioni tecniche, redatte a supporto dei rischi di mansione, atte a valutare o i rischi presenti nei vari ambienti riferibili alla generalità dei presenti (ad es. rischio incidente rilevante, etc.,) o rischi specifici e ben definiti ma relativi ad un esiguo numero di mansioni

- Ai fini della gestione delle emergenze, della prevenzione degli incendi e dell'evacuazione dei lavoratori, nonché per il caso di pericolo grave e immediato, devono essere adottate adeguate misure, che prevedano:

    - Lo svolgimento e la documentazione di periodiche prove di evacuazione ossia delle simulazioni ove vengono provate le interazioni fra le varie strutture aziendali preposte, le modalità di evacuazione, le modalità di comunicazione, etc.,
    - La definizione e adozione di adeguate misure per il controllo di situazioni di rischio in caso di emergenza, con particolare riferimento all'elaborazione e periodico aggiornamento, a cura del Servizio di Protezione e Prevenzione, del Piano di sicurezza e di gestione dell'emergenza, testato periodicamente
    - L'identificazione di lavoratori incaricati dell'attuazione delle misure di primo soccorso, gestione delle emergenze e antincendio che intervengono in funzione dell'area oggetto dell'emergenza
    - La programmazione delle verifiche e delle manutenzioni relative alle apparecchiature antincendio e la regolare tenuta Registro dell'Antincendio

- Devono essere organizzati i necessari rapporti con i servizi pubblici competenti in materia di pronto soccorso, salvataggio, lotta antincendio e gestione delle emergenze

- A seguito della valutazione dei rischi e secondo il programma di sorveglianza sanitaria devono essere individuate, in collaborazione con il medico competente e SPP, le mansioni che necessitano di sorveglianza sanitaria periodica, con

riferimento ai requisiti espressamente stabiliti dalla legge, ovvero risultanti da altri criteri/metodologie disponibili

- Gli infortuni sul lavoro che comportano un'assenza di almeno un giorno devono essere tempestivamente, accuratamente e cronologicamente annotati in apposito registro, redatto conformemente al modello approvato con Decreto del Ministero del Lavoro

- Devono essere predisposte apposite procedure interne volte a definire le modalità ed i termini per l'acquisizione e la trasmissione dei dati informativi relativi agli infortuni sul lavoro

- Deve essere definito, documentato, monitorato e periodicamente aggiornato, un programma di informazione dei lavoratori in materia di salute e sicurezza sul lavoro. Gli argomenti dell'informazione sono definiti anche in base alle risultanze della valutazione dei rischi e riguardano almeno:

  - I rischi per la salute e sicurezza connessi all'attività dell'impresa in generale
  - Le misure e le attività di protezione e prevenzione adottate
  - I rischi specifici cui il lavoratore è esposto in relazione all'attività svolta, le normative di sicurezza e le disposizioni aziendali in materia
  - Le procedure che riguardano il pronto soccorso, la lotta antincendio, l'evacuazione dei lavoratori
  - I nominativi del responsabile del servizio di prevenzione e protezione e del medico competente
  - I nominativi dei lavoratori incaricati di applicare le misure lotta all'incendio, evacuazione dei lavoratori e pronto soccorso

A ciascun lavoratore è inoltre fornita, per quanto di competenza, l'informazione specifica per quanto riguarda:

  - Uso delle attrezzature di lavoro
  - Uso dei dispositivi di protezione individuale
  - Movimentazione manuale dei carichi
  - Utilizzo di VDT
  - Segnaletica visuale, gestuale, vocale, luminosa e sonora
  - Ogni altro fattore di rischio e argomento rilevante ai fini della SSL individuato e definito nel programma di informazione

- Deve essere redatto, documentato, implementato, monitorato ed aggiornato un programma di formazione ed addestramento periodico, con particolare riguardo ai lavoratori neo-assunti, per i quali è necessaria una particolare qualificazione in materia di SSL. La formazione e l'addestramento devono essere differenziati in base al posto di lavoro e alle mansioni affidate ai lavoratori, nonché erogati anche in occasione dell'assunzione, del trasferimento o del cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro o di nuove tecnologie. Devono essere

monitorati ed adeguatamente documentati il regolare svolgimento e la partecipazione ai corsi di in materia di SSL

- Deve essere attuato il coinvolgimento di tutti i lavoratori sui temi della SSL con continuità e periodicità

- L'efficacia e l'adeguatezza delle misure di prevenzione e protezione devono essere periodicamente monitorate. Tali misure devono essere sostituite, modificate o aggiornate qualora ne sia riscontrata l'inefficacia e/o l'inadeguatezza, ovvero in relazione ad eventuali mutamenti organizzativi e dei rischi. È necessario predisporre un piano di esecuzione delle verifiche, che indichi anche le modalità di esecuzione delle stesse, nonché le modalità di segnalazione di eventuali difformità

- Il corretto utilizzo, da parte dei lavoratori, dei dispositivi di protezione individuale per lo svolgimento delle mansioni loro attribuite deve essere costantemente monitorato

- Il DDL e il RSPP con la partecipazione del Medico competente, devono programmare ed effettuate apposite riunioni con i RLS, volte ad approfondire le questioni connesse alla prevenzione ed alla protezione dai rischi. Le riunioni devono essere adeguatamente formalizzate mediante la redazione di apposito verbale, il quale dovrà essere inviato all'Organismo di Vigilanza (ODV)

- Il divieto di fumare in tutti gli ambienti di lavoro deve essere formalizzato ed adeguatamente pubblicizzato

- Deve essere garantita la manutenzione ordinaria e straordinaria dei dispositivi di sicurezza aziendale (ad esempio, porte tagliafuoco, lampade di emergenza, estintori, etc.,). Manutenzioni ordinarie programmate devono essere effettuate sugli ambienti, gli impianti, i macchinari e le attrezzature generiche e specifiche in conformità alle indicazioni dei fabbricanti

- Deve essere predisposto ed implementato un sistema di controllo interno idoneo a garantire la costante registrazione, anche attraverso l'eventuale redazione di apposita documentazione, delle verifiche svolte dalla Società in materia di SSL. In tale ambito, la Società deve prevedere che l'ODV effettui un'attività di monitoraggio periodica della funzionalità del complessivo sistema preventivo adottato. A tal fine deve essere inviata all'ODV copia della reportistica periodica in materia di SSL, del verbale della riunione periodica di cui all'art. 35 del D.Lgs. 81/08 e succ. mod, nonché tutti i dati relativi agli infortuni sul lavoro occorsi nei siti della Società

- Devono essere previste nel sistema disciplinare e meccanismo sanzionatorio adottato dalla Società, nel rispetto di quanto previsto dalla legge e dalla contrattazione collettiva, apposite sanzioni per la violazione del Modello in materia di SSL

La Società ha facoltà di integrare, in qualsiasi momento, i principi elencati nel presente paragrafo così come le procedure

aziendali vigenti, qualora ritenuto opportuno al fine di garantire la SSL

Si riportano qui di seguito gli adempimenti che, in attuazione dei principi sopra descritti e della normativa applicabile, sono posti a carico delle figure rilevanti, salvo l'obbligo in capo a tutti i destinatari di segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso

Il Datore di Lavoro

Al datore di lavoro sono attribuiti tutti gli obblighi in materia di salute e sicurezza sul lavoro, tra cui i seguenti compiti non delegabili:

- Valutare tutti i rischi per la sicurezza e per la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari (es. rischi connessi alla differenza di genere, alla provenienza da altri Paesi, etc.,) anche nella scelta delle attrezzature di lavoro, nonché nella sistemazione dei luoghi di lavoro; a tal riguardo, nelle scelte operate il Datore di Lavoro dovrà garantire il rispetto degli standard tecnico-strutturali previsti dalla legge

- Elaborare, all'esito di tale valutazione, un Documento di Valutazione dei Rischi con data certa contenente:
  - Una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro, nella quale siano specificati i criteri adottati per la valutazione stessa
  - L'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuale adottati, a seguito della suddetta valutazione dei rischi
  - Il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza
  - L'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere
  - L'indicazione del nominativo del RSPP, degli RLS e del medico competente che abbiano partecipato alla valutazione del rischio
  - L'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento

L'attività di valutazione e di redazione del documento deve essere compiuta in collaborazione con il RSPP e con il medico competente. La valutazione dei rischi è oggetto di consultazione preventiva con il RLS, e va nuovamente effettuata in occasione di modifiche del processo produttivo significative ai fini della sicurezza e della salute dei Lavoratori, o in relazione al grado di evoluzione della tecnica, della prevenzione e della protezione, a seguito di infortuni significativi o quando i risultati della Sorveglianza Sanitaria ne evidenzino la necessità

Nell'ambito della riunione annuale ai fini della sicurezza a cui partecipano il Datore di Lavoro, il RSPP, il Medico Competente, gli RLS viene riesaminato, tra gli altri documenti, anche il Documento di Valutazione dei Rischi

- Designare il Responsabile del Servizio di Prevenzione e Protezione sia esso interno o esterno all'azienda

Al Datore di Lavoro sono attribuiti i seguenti altri compiti dallo stesso delegabili a soggetti qualificati. Tali compiti, previsti dal Decreto Sicurezza, riguardano, tra l'altro, il potere di:

- Nominare il medico competente per l'effettuazione della sorveglianza sanitaria
- Designare preventivamente i Lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione delle emergenze
- Fornire ai Lavoratori i necessari ed idonei dispositivi di protezione individuale, sentito il RSPP ed il medico competente
- Adottare le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico
- Adempiere agli obblighi di informazione e formazione di cui ai successivi paragrafi
- Comunicare all'Inail, a fini statistici e informativi, i dati relativi agli infortuni sul lavoro che comportino un'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, le informazioni relative agli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni
- Convocare la riunione periodica di cui all'art. 35 del Decreto Sicurezza;
- Aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione
- Prevedere un adeguato sistema di vigilanza sul rispetto delle procedure e delle misure di sicurezza da parte dei lavoratori, individuando specifiche figure a ciò deputate
- Adottare provvedimenti disciplinari, in conformità alle disposizioni contrattuali e legislative, nei confronti dei lavoratori che non osservino le misure di prevenzione e le procedure di sicurezza mettendo in pericolo, attuale o potenziale, la propria o altrui sicurezza

In relazione a tali compiti, ed a ogni altro compito affidato al datore di lavoro che possa essere da questi delegato ai sensi del Decreto Sicurezza, la suddetta delega, cui deve essere data adeguata e tempestiva pubblicità, è ammessa con i seguenti limiti e condizioni:

- Che essa risulti da atto scritto recante data certa
- Che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate
- Che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate
- Che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate
- Che la delega sia accettata dal delegato per iscritto

Al fine di garantire l'attuazione di un modello di sicurezza aziendale sinergico e compartecipativo, il datore di

lavoro fornisce al Servizio di Prevenzione e Protezione e al Medico Competente informazioni in merito a:

- La natura dei rischi
- L'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive
- La descrizione degli impianti e dei processi produttivi
- I dati relativi agli infortuni e quelli relativi alle malattie professionali

Il Servizio di Prevenzione e Protezione (SPP)

Nell'adempimento degli obblighi in materia di salute e sicurezza sul lavoro, il Datore di Lavoro organizza il Servizio di Prevenzione e Protezione all'interno dell'azienda o incarica persone o servizi esterni assicurandosi che gli ASPP ed i RSPP, da questi nominati, siano in possesso delle capacità e dei requisiti professionali di cui all'Art. 32 del Decreto Sicurezza (es. possesso di un titolo di studio di istruzione secondaria superiore, nonché di un attestato di frequenza, con verifica di apprendimento, a specifici corsi di formazione adeguati alla natura dei rischi presenti sul luogo di lavoro, etc.,)

Il SPP provvede a:

- Individuare i fattori di rischio, valutare i rischi e individuare le misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente e sulla base della specifica conoscenza dell'organizzazione aziendale
- Elaborare, per quanto di competenza, le misure preventive e protettive di cui all'art. 28 del Decreto Sicurezza e dei sistemi di controllo di tali misure
- Elaborare procedure di sicurezza per le varie attività aziendali
- Proporre programmi di informazione e formazione dei lavoratori
- Partecipare, attraverso il RSPP, alla "riunione periodica di prevenzione e protezione dai rischi" di cui all'art. 35 del Decreto Sicurezza
- Partecipare alle consultazioni in materia di tutela della salute e della sicurezza
- Informare i lavoratori, a nome e per conto del Datore di Lavoro, sulle tematiche di cui all'art. 36 del Decreto Sicurezza come indicato nel dettaglio al successivo paragrafo
- Segnalare all'Organismo di Vigilanza la sussistenza di eventuali criticità nell'attuazione delle azioni di recupero prescritte dal Datore di Lavoro

L'eventuale sostituzione del RSPP deve essere comunicata all'Organismo di Vigilanza con l'espressa indicazione delle motivazioni a supporto di tale decisione

Il Medico Competente

Il Medico Competente deve essere in possesso di uno dei titoli di cui all' art. 38 del Decreto Sicurezza e, precisamente:

- Specializzazione in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica
- Docenza in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica, o in tossicologia industriale, o in igiene industriale, o in fisiologia ed igiene del lavoro o in clinica del lavoro
- Autorizzazione di cui all'articolo 55 del D.Lgs. 277/91 e successive modifiche che prevede una comprovata esperienza professionale di almeno 4 anni

Il Medico Competente provvede a:

- Collaborare con il Datore di Lavoro e con il Servizio di Prevenzione e Protezione alla predisposizione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori
- Effettuare le visite mediche preventive e periodiche previste dalla legge e da programmi di prevenzione opportunamente stabiliti
- Fornire informazioni ai lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti ed informarli sui risultati
- Esprimere il giudizio di idoneità specifica alla mansione
- Istituire ed aggiornare, per ogni lavoratore sottoposto a sorveglianza sanitaria, le cartelle sanitarie e di rischio, con salvaguardia del segreto professionale
- Visitare gli ambienti di lavoro, congiuntamente al RSPP, redigendo specifico verbale e partecipare alla programmazione del controllo dell'esposizione dei lavoratori
- Comunicare, in occasione della "riunione periodica di prevenzione e protezione dai rischi" di cui all'art. 35 del Decreto Sicurezza, i risultati anonimi collettivi degli accertamenti sanitari, fornendo le informazioni necessarie
- Collaborare all'attività di informazione e formazione dei lavoratori
- Collaborare con il Datore di Lavoro alla predisposizione del servizio di pronto soccorso

Il Medico Competente può avvalersi, per accertamenti diagnostici, della collaborazione di medici specialisti scelti in accordo con il Datore di Lavoro che ne sopporta gli oneri.

Il Datore di Lavoro assicura al Medico Competente le condizioni necessarie per lo svolgimento di tutti i suoi compiti garantendone la piena autonomia.

I Rappresentanti dei Lavoratori per la Sicurezza (RLS)

Sono i soggetti eletti o designati, in conformità a quanto previsto dagli accordi sindacali in materia, per rappresentare i lavoratori per gli aspetti di salute e sicurezza sui luoghi di lavoro

Gli RLS

- Accedono ai luoghi di lavoro
- Sono consultati preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive
- Sono consultati sulla designazione del RSPP, degli ASPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso
- Sono consultati in merito all'organizzazione delle attività formative
- Promuovono l'elaborazione, l'individuazione a l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei Lavoratori
- Partecipano alla "riunione periodica di prevenzione e protezione dai rischi" di cui all'art. 35 del Decreto Sicurezza
- Ricevono informazioni e la documentazione aziendale inerenti alla valutazione dei rischi e le misure di prevenzione relative, nonché quelli inerenti alle sostanze e ai preparati pericolosi, alle macchine, agli impianti, all'organizzazione e agli ambienti di lavoro, agli infortuni ed alle malattie professionali; ricevono altresì, su loro richiesta e per l'espletamento delle loro funzioni, copia del Documento di Valutazione dei Rischi
- Ricevono informazioni provenienti dai servizi di vigilanza
- Ricevono un'informazione adeguata e comunque non inferiore a quella prevista per i lavoratori ai sensi dell'art. 37 del Decreto Sicurezza
- Formulano osservazioni in occasione di visite e verifiche effettuate dalle autorità competenti dalle quali siano sentiti
- Avvertono il Datore di Lavoro dei rischi individuati nel corso della loro attività
- Possono far ricorso alle autorità competenti qualora ritengano che le misure di prevenzione e protezione dai rischi adottate dal Datore di Lavoro o dai dirigenti ed i mezzi impiegati per attuarle non siano idonei a garantire la sicurezza e la salute durante il lavoro

Gli RLS dispongono del tempo necessario allo svolgimento dell'incarico, senza perdita di retribuzione, nonché dei mezzi e degli spazi necessari per l'esercizio delle funzioni e delle facoltà loro riconosciute; non possono subire pregiudizio alcuno a causa dello svolgimento della propria attività e nei loro confronti si applicano le stesse tutele previste dalla legge per le rappresentanze sindacali

I Lavoratori

È cura di ciascun lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite

I lavoratori devono:

- Osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale
- Utilizzare correttamente i macchinari, le apparecchiature, gli utensili, i mezzi di trasporto e le altre attrezzature di lavoro, nonché gli eventuali dispositivi di sicurezza
- Segnalare immediatamente al Datore di Lavoro, al Dirigente o al Preposto le deficienze dei mezzi e dispositivi dei punti precedenti, nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli, dandone notizia al Rappresentante dei Lavoratori per la Sicurezza
- Non rimuovere né modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo
- Non compiere di propria iniziativa operazioni né manovre che non siano di loro competenza ovvero che possano compromettere la sicurezza propria o di altri lavoratori
- Sottoporsi ai controlli sanitari previsti nei loro confronti
- Contribuire, insieme al Datore di Lavoro, ai Dirigenti e ai Preposti, all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro

4.9 - Attività di formazione ed informazione

ATTIVITÀ DI INFORMAZIONE

L'azienda è tenuta a fornire adeguata informazione ai dipendenti e nuovi assunti, ai lavoratori, agli stagisti circa:

- I rischi specifici dell'impresa
- Le conseguenze derivanti dallo svolgimento della propria attività non conformemente alle prescrizioni di legge e di autoregolamentazione di cui l'azienda si è dotata
- Il ruolo e responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità delle prescrizioni di cui sopra
- Le misure di prevenzione e protezione adottate nonché sulle conseguenze che il mancato rispetto di tali misure può provocare anche ai sensi del D.Lgs. 231/2001.

Tale informazione deve essere facilmente comprensibile per ciascun lavoratore, consentendo a ciascuno di acquisire le necessarie conoscenze e deve essere preceduta, qualora riguardi lavoratori immigrati, dalla verifica della comprensione della lingua utilizzata nel percorso formativo

Ciò premesso, l'azienda, in considerazione dei diversi ruoli, responsabilità, capacità e dei rischi cui è esposto ciascun dipendente, fornisce tra l'altro, adeguata informazione ai lavoratori sulle seguenti tematiche:

- Sui rischi per la salute e sicurezza sul lavoro, connessi all'attività dell'impresa in generale e su quelli specifici cui ciascun lavoratore è esposto in relazione all'attività svolta
- Sulle misure di prevenzione e protezione adottate
- Sulle procedure che riguardano il primo soccorso, la lotta antincendio, l'evacuazione dei luoghi di lavoro
- Sui nominativi dei lavoratori incaricati delle misure di emergenza e di pronto soccorso, nonché del Medico Competente

Si precisa infine che nei confronti dei dipendenti distaccati se esistenti, in capo ai quali permangono gli obblighi in materia di prevenzione e protezione, la società destina adeguata informativa circa i rischi generalmente connessi alle mansioni per le quali i dipendenti vengono distaccati

La società organizza altresì periodici incontri tra le funzioni preposte alla sicurezza sul lavoro fornendone comunicazione all'Organismo di Vigilanza

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, eventualmente anche mediante apposita verbalizzazione. A tali fini la società deve mettere a disposizione dei destinatari una bacheca che conterrà i vari riferimenti in tema di sicurezza, la normativa, la descrizione della struttura, le circolari interne ed i nominativi degli RLS

ATTIVITÀ DI FORMAZIONE

La società deve fornire adeguata formazione a tutti i lavoratori in materia di sicurezza sul lavoro e il contenuto della stessa deve essere facilmente comprensibile e consentire di acquisire le conoscenze e competenze necessarie

A tal riguardo si specifica che:

- Il RSPP e il medico competente debbono partecipare alla stesura del piano di formazione
- La formazione erogata deve prevedere questionari di valutazione dell'apprendimento
- La formazione deve essere adeguata ai rischi della mansione cui il lavoratore è in concreto assegnato
- I lavoratori che cambiano mansione e quelli trasferiti devono fruire di formazione specifica, preventiva e/o aggiuntiva, ove necessario, per il nuovo incarico
- Ciascun lavoratore deve essere sottoposto a tutte quelle azioni formative rese obbligatorie dalla legge, tra le quali, ad esempio:

    - L'uso delle attrezzature di lavoro
    - La movimentazione manuale carichi
    - L'uso dei videoterminali
    - La segnaletica visuale, gestuale, vocale, luminosa e sonora

- Gli addetti a specifici compiti in materia di emergenza devono ricevere specifica formazione
- L'azienda deve effettuare periodiche esercitazioni di emergenza di cui deve essere data evidenza (attraverso, ad esempio, la verbalizzazione dell'avvenuta esercitazione con riferimento alle modalità di svolgimento e alle risultanze)
- I neo assunti - in assenza di pregressa esperienza professionale/lavorativa e di adeguata qualificazione - non possono essere adibiti in autonomia ad attività operativa ritenuta più a rischio infortuni se non dopo l'acquisizione di un grado di professionalità idoneo allo svolgimento della stessa mediante adeguata formazione non inferiore ad almeno tre mesi dall'assunzione, salvo periodi più ampi per l'acquisizione di qualifiche specifiche

Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, eventualmente anche mediante apposita verbalizzazione

4.10 - Istituzione di flussi informativi

Con l'obiettivo di rafforzare l'efficacia del sistema organizzativo adottato dalla società per la gestione della salute e sicurezza dei Lavoratori e quindi per la prevenzione degli infortuni, la società si organizza per assicurare un adeguato livello di circolazione e condivisione delle informazioni tra tutti i lavoratori

In primo luogo, la società mette a disposizione un apposito sistema di comunicazione aziendale attraverso cui ciascun Lavoratore ha la possibilità di conoscere le procedure aziendali in tema di sicurezza e portare a conoscenza del proprio superiore gerarchico le proprie osservazioni, proposte ed esigenze di miglioramento relative alla gestione della salute e sicurezza in ambito aziendale

In secondo luogo, la società garantisce a tutti i lavoratori un'adeguata e costante informativa attraverso la predisposizione di comunicati e l'organizzazione di incontri periodici, cui l'Organismo di Vigilanza ha la facoltà di partecipare, che abbiano ad oggetto:

- Eventuali nuovi rischi in materia di salute e sicurezza
- Modifiche nella struttura organizzativa per la gestione della salute e sicurezza nei luoghi di lavoro
- Predisposizione di nuove procedure o aggiornamento in merito a quelle esistenti per la gestione della salute e sicurezza sul lavoro
- Ogni altro aspetto inerente la salute e sicurezza dei lavoratori

4.11 - Conservazione della documentazione rilevante

La società garantisce che vengano adeguatamente conservati su supporto cartaceo ed informatico, e aggiornati i seguenti documenti:

- La cartella sanitaria, ove prevista, deve essere istituita e aggiornata dal medico competente e custodita dal Datore di Lavoro
- Il registro infortuni
- Verbalizzazione delle visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal medico competente
- Documenti che registrano gli adempimenti espletati in materia di sicurezza e salute sul lavoro
- Documento di Valutazione dei Rischi
- Documento di Valutazione dei Rischi integrato ("DUVRI")
- Nomina formale del Responsabile e degli Addetti al Servizio di Prevenzione e Protezione (RSPP e ASPP), del Medico Competente, degli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, nonché degli eventuali Dirigenti e Preposti
- Documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti alla realtà aziendale
- Documentazione inerente a regolamenti ed accordi aziendali
- Manuali di istruzione per l'uso di macchine e attrezzature forniti da fabbricanti e/o fornitori
- Ogni procedura adottata dall'azienda per la gestione della salute e sicurezza sui luoghi di lavoro
- Tutta la documentazione relativa alle attività di cui a "Informazione" e "Formazione", che deve essere conservata a cura del RSPP e messa a disposizione dell'Organismo di Vigilanza

4.12 - Contratto di appalto

La società predispone e mantiene aggiornato l'elenco delle aziende che operano all'interno dei propri siti con contratto d'appalto

Le modalità di gestione e di coordinamento dei lavori in appalto vengono formalizzate in contratti scritti nei quali siano presenti espressi riferimenti agli adempimenti in capo al Datore di Lavoro di cui all'art. 26 del Decreto Sicurezza, tra cui, in via esemplificativa:

- Verificare l'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori da affidare in appalto attraverso:
  - Acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato
  - Acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico professionale ai sensi dell'articolo 4 del Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445
- Fornire informazioni dettagliate agli appaltatori circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività
- Cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto

- Coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori
- Predisporre un unico DUVRI che indichi le misure adottate al fine di eliminare, o quanto meno ridurre al minimo, i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva; tale documento deve allegarsi al contratto di appalto o d'opera
- Verificare in fase di gestione del contratto ed esecuzione dei lavori il rispetto delle misure previste di prevenzione e protezione e il rispetto degli adempimenti di legge verso il personale di cui al punto precedente
- Assicurarsi che il personale dell'impresa appaltatrice o subappaltatrice esponga, in presenza dello specifico obbligo di legge, la tessera di riconoscimento con fotografia, dati anagrafici e indicazione del Datore di Lavoro

Nei contratti di somministrazione, di appalto e di subappalto, vengono specificamente indicati i costi relativi alla sicurezza del lavoro

A tali dati possono accedere, su richiesta, gli RLS e le organizzazioni sindacali dei lavoratori

Infine, nei contratti di appalto viene chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto

CLAUSOLE CONTRATTUALI

La società inserisce, nei contratti con i Collaboratori esterni e con i Partner, un'apposita dichiarazione dei medesimi con cui afferma:

- Di essere a conoscenza della normativa di cui al Decreto e delle sue implicazioni per la società, nonché dell'adozione da parte della stessa del Modello e del Codice Etico
- Di non essere mai stati implicati in procedimenti giudiziari relativi ai reati contemplati nel Decreto
- Di impegnarsi al rispetto delle prescrizioni contenute nel Decreto, nonché dei principi contenuti nel Modello, nel Codice Etico

Inoltre, nei contratti con i collaboratori esterni e con i partner, viene inserita un'apposita clausola che regola le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto nonché dei principi di cui al Modello (ad es. clausole risolutive espresse, penali)

PRINCIPI PROCEDURALI SPECIFICI

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale i dipendenti sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:

- Organigramma aziendale
- Documento di Valutazione dei Rischi con i relativi documenti integrativi
- Procedure interne di selezione, qualificazione e monitoraggio dei fornitori di servizi
- Procedure interne finalizzate a garantire il mantenimento di elevati standard di sicurezza nei lavori appaltati a terzi a tutela sia del personale dell'azienda che di quello delle ditte appaltatrici presso la sede aziendale
- Procedure interne per l'informazione e la formazione del personale in materia di tutela della salute e della sicurezza sul lavoro
- Codice Etico

Tali procedure e i documenti devono essere considerati come parte integrante delle strutture di organizzazione gestione e controllo necessarie per il corretto funzionamento ed efficacia del Modello 231 e sono aggiornati dalle funzioni aziendali e dagli Organi Sociali competenti

4.13 – Gestione dell'emergenza sanitaria Covid-19 in azienda

La diffusione del virus COVID-19, anche noto come *"coronavirus"*, impone l'adozione di specifiche, ulteriori, cautele a tutela del lavoratore le cui prestazioni non siano cessate nel corso dell'emergenza sanitaria. Si raccomanda, sul punto, l'attenta lettura dei D.P.C.M. 11 marzo 2020, D.P.C.M. 22 marzo 2020 e D.P.C.M. 10 aprile 2020, che disciplinano la sospensione di numerose attività commerciali/imprenditoriali (sino alla data del 3 maggio 2020, per effetto del D.P.C.M. da ultimo richiamato). Resta, peraltro, applicabile le misure di contenimento più restrittive adottate dalle Regioni (cfr. art. 8, comma III, D.P.C.M. 10 aprile 2020).
Nell'ipotesi in cui l'attività non sia oggetto di sospensione generalizzata, sono doverosi:
1) la rigorosa osservanza delle norme di comportamento previste dal D.P.C.M. 11 marzo 2020, dal D.P.C.M. 22 marzo 2020 e dal D.P.C.M. 10 aprile 2020. Sul punto, si segnala che gli allegati 4 e 5 del D.P.C.M. 10 aprile 2020 dettano specifiche norme igienico-sanitarie da adottare. Si segnala, ancora, che il D.P.C.M. 10 aprile 2020, unitamente alla precedente normativa emergenziale, prevede e raccomanda l'impiego di modalità di lavoro agile e la fruizione dei periodi di congedo ordinario di ferie;
2) il compimento, attraverso gli organi a ciò preposti, di una valutazione in ordine al nuovo rischio aziendale di diffusione del COVID-10;
3) in ogni caso, si raccomanda **l'osservanza del Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19** negli ambienti di lavoro, siglato il 14 marzo 2020 (da Governo, Confindustria, Confapi, Confartigianato, CGIL, CISL e UIL), contenente misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro, per agevolare le imprese nell'adozione di protocolli di sicurezza anti-contagio e per consentire la prosecuzione delle attività produttive in presenza di condizioni che assicurino alle persone che lavorano adeguati livelli di protezione.
Detto Protocollo è stato oggetto di integrazione con diversi provvedimenti successivi, alla cui compliance relativa alla salute e sicurezza sul lavoro, si rimanda.

PARTE SPECIALE – SEZ. C – REATI DI OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

(*Art. 25-septies del D.Lgs. 231/01*)

MOGC-SPE-03

Digitronica.IT al fine di garantire la tutela della salute e sicurezza sui luoghi di lavoro si è dotata in data 04 maggio 2020 di un proprio Protocollo di Sicurezza Aziendale Anti contagio Covid-19, sottoscritto da:

- Datore di lavoro
- RSPP
- RLS
- Preposto
- Medico Competente.

Per le specifiche misure adottate si rimanda interamente al Protocollo che si ritiene, fino alla dichiarazione ufficiale da parte degli organi governativi di fine dell'epidemia, parte integrante del Modello e la cui inosservanza produce i medesimi effetti dell'inosservanza delle misure esplicitate nei paragrafi precedenti.

Il citato Protocollo fornisce **regole generali di comportamento ai dipendenti**, qui si riportano le principali:

- Sono stati nominati 4 incaricati a tale rilevazione ed è fornita adeguata informativa sul trattamento dei dati personali ai sensi dell'art. 13 del Regolamento UE 2016/679;
- Prima dell'accesso sul luogo di lavoro viene rilevata la temperatura, se superiore a 37.5° è interdetto l'accesso;
- il dipendente cui è interdetto l'accesso viene isolato e invitato a contattare il proprio medico medico curante;
- il personale è informato del divieto di accesso in azienda a chiunque, nei 14 giorni precedenti, abbia avuto contatti con soggetti positivi al Covid-19 o provenga dalle cd. "zone rosse";
- l'ingresso in azienda da parte di soggetti risultati positivi potrà avvenire unicamente previa comunicazione avente ad oggetto certificazione medica da cui risulti la avvenuta negativizzazione del tampone;
- la consegna di materiali e prodotti da parte die fornitori avviene unicamente al piano precludendo l'ingresso in azienda al fornitore stesso;
- nelle fasi di consegna dovranno essere evitati contatti, mantenendo in ogni caso la distanza minima di 1 metro ed indossando sempre i DPI;
- nel caso in cui l'accesso del fornitore in azienda sia indispensabile, dovrà essere sempre previamente autorizzata al Datore di Lavoro e/o dal Preposto autorizzato;
- non è permesso l'accesso nei locali aziendali ai visitatori, se ritenuto necessario dovrà essere sempre previamente autorizzata al Datore di Lavoro e/o dal Preposto autorizzato;
- sono riorganizzate le fasi di lavoro per i dipendenti di aziende terze che forniscono servizi a Digitronica.IT (es. addetti pulizie e manutenzione) in modo da evitare contatti;
- la Società provvede alla pulizia giornaliera ed alla sanificazione periodica dei propri locali, attrezzature, auto di servizio e auto a noleggio;
- il datore di lavoro verifica l'avvenuta sanificazione e fornisce specifici kit detergenti che rende disponibili in azienda;
- in caso di presenza di una persona positiva in azienda si procede alla sanificazione e pulizia dei locali ai sensi della circolare n. 5443 del 22 febbraio 2020 del Ministero della Salute;
- le azioni di sanificazione devono prevedere attività eseguite utilizzando prodotti aventi le caratteristiche contenute nella circolare n. 5443 del 22 febbraio 2020;
- chiunque in azienda è tenuto ad indossare la mascherina, detergere spesso le mani con gel igienizzante e mantenere

la distanza interpersonale di almeno 1 metro;
- l'accesso agli spazi comuni è contingentato e per un tempo di sosta ridotto con il mantenimento della distanza di sicurezza di almeno 1 metro;

Inoltre, nel Protocollo, l'azienda promuove le seguenti misure a livello di organizzazione aziendale:
- promuovere l'utilizzo dello smart working ove possibile;
- procedere ad una rimodulazione dei livelli produttivi;
- assicurare la turnazione dei dipendenti;
- utilizzare gli ammortizzatori sociali, la fruizione di ferie e permessi per consentire l'astensione dal lavoro;
- gli interventi fuori sede saranno autorizzati sa specifici ordini di servizio;
- il personale in trasferta osserva il Protocollo;
- sono consentite le riunioni in presenza solo se urgenti ed indifferibili, garantendo sempre il rispetto del Protocollo;
- la formazione deve avvenire unicamente con modalità a distanza;

Nel caso in cui ci sia una persona sintomatica in azienda, questa è tenuta a comunicarlo immediatamente al DdL e/o al Preposto e/o al RLS. Il soggetto viene subito isolato e l'Azienda ne informa le autorità sanitarie competenti e collabora nella definizione di eventuali contatti stretti.

La sorveglianza sanitaria è garantita a condizione che al Medico Competente sia consentito operare nel pieno rispetto del Protocollo previlegiando unicamente le visite con carattere di urgenza ed indifferibilità.

4.14 - I controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei destinatari, nei limiti dei rispettivi compiti e attribuzioni, delle regole e principi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo

Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate in tema di sicurezza sul lavoro, la documentazione prevista dal Decreto Sicurezza, il rispetto delle relative formalità, nonché l'adeguatezza dei sistemi dei controlli interni adottati in tale ambito

In particolare l'Organismo di Vigilanza dovrà esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute

Al fine di svolgere i propri compiti, l'Organismo di Vigilanza può:

- Partecipare agli incontri organizzati dalla società tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti
- Accedere a tutta la documentazione di cui al precedente paragrafo

L'azienda istituisce altresì a favore dell'Organismo di Vigilanza flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte

L'Organismo di Vigilanza, nell'espletamento delle attività di cui sopra, può avvalersi di tutte le risorse competenti in azienda. L'Organismo di Vigilanza può incontrarsi o chiedere documentazione al RSPP in relazione agli aspetti relativi alle tematiche di salute e sicurezza sul lavoro.

☑ **Sistema di gestione**
- ☑ *Modello di organizzazione*
- ☐ *Codice etico*
- ☐ *Analisi dei rischi*

☐ **Procedure**

☐ **Modulistica**

Digitronica.IT
Your Security Our Software

PARTE SPECIALE – SEZ. D – REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI
(*Art. 24-bis del D.Lgs. 231/01*)

MOGC-SPE-04

Organizzazione

Digitronica.IT S.p.A.

Sede: Viale del Lavoro, 52 Verona
Phone: 045 50 19 01
Fax: 045 50 22 58
Email: info@digitronica.it
Pec: digitronica.it@pec.it

MOGC 231 – PARTE SPECIALE

ai sensi del D.Lgs. n. **231** del 8 Giugno 2001 e s.m.i.

Master	☐
Copia controllata	☐
Copia non controllata	☐
Numero della copia	

Emissione DG	Data		Firma	
Approvazione DG	Data		Firma	
Approvazione ODV	Data		Firma	

Stato delle revisioni

Versione	Data	Descrizione	Autore
00	*04/06/2019*	Prima emissione	Digitronica.IT Srl
01	*01/12/2020*	Aggiornamento	Digitronica.IT S.p.A.
02	*01/04/2022*	Aggiornamento	Digitronica.IT S.p.A.
03	*22/01/2024*	Aggiornamento OdV	Digitronica.IT SpA

Indice generale della sezione

Modello di Organizzazione, Gestione e Controllo – Parte speciale

5.1 - Introduzione e funzione della parte speciale dei reati informatici e di trattamento illecito dei dati

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Dipendenti e dagli Organi Sociali aziendali, nonché dai suoi Collaboratori esterni e dai Partner come già definiti nella Parte Generale

Obiettivo della presente Parte Speciale e che tutti i Dipendenti e gli altri soggetti eventualmente autorizzati adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi degli illeciti in essa considerati Nello specifico, la presente Parte Speciale ha lo scopo di:

- Indicare i principi procedurali e le regole di comportamento che i Dipendenti e gli altri soggetti eventualmente autorizzati sono chiamati ad osservare ai fini della corretta applicazione del Modello

- Fornire all'Organismo di Vigilanza, nonché ai responsabili delle altre funzioni aziendali che cooperano con lo stesso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica

La società adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione dei reati di seguito descritti

5.2 - Criteri per la definizione dei reati informatici e di trattamento illecito dei dati

Ad integrazione delle definizioni elencate nella Parte Generale del Modello, si consideri la seguente ulteriore definizione da applicare alla presente Parte Speciale:

"**Delitti Informatici**": sono i delitti richiamati dall'art. 24-bis del Decreto e disciplinati dal codice penale agli artt. 491-bis, 615-ter, 615-quater, 615-quinquies, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies e 640-quinquies
L'**articolo 167** del Codice in materia di protezione dei dati personali, cosi come aggiornato dal D.lgs. 101/2018, prevede che sia punito, salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri **profitto** ovvero di arrecare **danno** all'interessato, arreca nocumento all'interessato in violazione di specifiche disposizioni di legge (come quelle che regolamentano il trattamento di dati ex art. 9 e il trasferimento internazionale dei dati personali). E' altresì punito chi, al fine di trarre per sè o per altri profitto o di arrecare danno all'interessato procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti, arreca nocumento all'interessato.

5.3 - Le fattispecie di reato richiamate dal D.Lgs. 231/01

La legge 18 marzo 2008, n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento intero" ha ampliato le

fattispecie di reato che possono generare la responsabilità delle società. L'art. 7 del predetto provvedimento ha introdotto nel Decreto l'art. 24 - bis "Delitti informatici e trattamento illecito di dati", che riconduce la responsabilità amministrativa degli enti ai reati individuati nelle sezioni seguenti

La presente Parte Speciale si riferisce ai Delitti informatici e trattamento illecito di dati (di seguito, per brevità, i "Delitti Informatici")

Si descrivono qui di seguito le singole fattispecie di reato per le quali l'art. 24-bis del D.Lgs. n. 231/2001 prevede una responsabilità degli enti nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio degli stessi

5.3.1 - Falsità in documenti informatici (Art. 491-bis c.p.)

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, co. 1, lett. p), D.Lgs. 82/2005, salvo modifiche ed integrazioni)

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di inserimento fraudolento di dati falsi nelle banche dati pubbliche oppure la condotta dell'addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli

Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente, allo scopo di eliminare le prove di un altro reato

A tal proposito il D.Lgs 7 del 15 gennaio 2016 aggiunge : " *Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici*"

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

Tale reato si realizza quando un soggetto "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 diritto ad escluderlo". Tale delitto è punito con la reclusione fino a tre anni

La pena è della reclusione da uno a cinque anni:

- 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
- se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato
- 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 il delitto in oggetto riguardi 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

Il delitto di accesso abusivo al sistema informatico rientra tra i delitti contro la libertà individuale. Il bene che viene protetto dalla norma è il domicilio informatico seppur vi sia chi sostiene che il bene tutelato è, invece, l'integrità dei dati e dei programmi contenuti nel sistema informatico. L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato

Il delitto di accesso abusivo a sistema informatico si integra, ad esempio, nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura)

Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della società accedendo abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), ad esempio, per prendere cognizione di dati riservati di un'impresa concorrente, ovvero tramite la manipolazione di dati presenti sui propri sistemi come risultato dei processi di business allo scopo di produrre un bilancio falso o, infine, mediante l'accesso abusivo a sistemi aziendali protetti da misure di sicurezza, da parte di utenti dei sistemi stessi, per attivare servizi non richiesti dalla clientela

5.3.3 -Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

Tale reato si realizza quando un soggetto, "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 di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo". Tale reato è punito con la reclusione sino ad un anno e con la multa sino a Euro 5.164

La pena è della reclusione da uno a due anni e della multa da Euro 5.164 a Euro 10.329 se il danno è commesso:

- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità
- 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, ovvero con abuso della qualità di operatore del sistema

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'art. 615-quater, pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.
I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (ad esempio, badge, carte di credito, bancomat e smart card)

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma, ovvero di una clausola contrattuale, che vieti detta condotta (ad esempio regolamento aziendale sull'utilizzo di Internet)

L'art. 615-quater, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza

Risponde, ad esempio, del delitto di diffusione abusiva di codici di accesso, il dipendente di un'azienda autorizzato ad un certo livello di accesso al sistema informatico che ottenga illecitamente il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno dell'azienda oppure carpisca in altro modo fraudolento o ingannevole il codice di accesso

5.3.4 - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinqies c.p.)

Tale reato si realizza qualora qualcuno, "allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici"

Tale reato è punito con la reclusione fino a due anni e con la multa sino a Euro 10.329

Questo delitto è integrato, ad esempio, nel caso in cui il soggetto si procuri un virus, idoneo a danneggiare un sistema

informatico o qualora si producano o si utilizzino delle smart card che consentono il danneggiamento di apparecchiature o di dispositivi elettronici

Questi fatti sono punibili solo nel caso in cui un soggetto persegua lo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati oppure i programmi in essi contenuti o, ancora, al fine di favorire l'interruzione parziale o totale o l'alterazione del funzionamento. Ciò si verifica, ad esempio, qualora un dipendente introduca un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico di un concorrente

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

Tale ipotesi di reato si integra qualora un soggetto "fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisce o interrompe tali comunicazioni", nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione al pubblico. Tale reato è punito con la reclusione da sei mesi a quattro anni

La pena è della reclusione da uno a cinque anni:

- 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
- se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato
- 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

La norma tutela la libertà e la riservatezza delle comunicazioni informatiche o telematiche durante la fase di trasmissione al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi

La fraudolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in cui la comunicazione sia rivolta ad un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente

quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione

Il reato si integra, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente

5.3.6 - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

Questa fattispecie di reato si realizza quando qualcuno, "fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi". Tale reato è punito con la reclusione da uno a quattro anni

La condotta vietata dall'art. 617-quinquies è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate. Si tratta di un reato che mira a prevenire quello precedente di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche

Anche la semplice installazione di apparecchiature idonee all'intercettazione viene punita dato che tale condotta rende probabile la commissione del reato di intercettazione. Ai fini della condanna il giudice dovrà, però, limitarsi ad accertare se l'apparecchiatura installata abbia, obiettivamente, una potenzialità lesiva

Qualora all'installazione faccia seguito anche l'utilizzo delle apparecchiature per l'intercettazione, interruzione, impedimento o rivelazione delle comunicazioni, si applicheranno nei confronti del soggetto agente, qualora ricorrano i presupposti, più fattispecie criminose

Il reato si integra, ad esempio, a vantaggio dell'ente, nel caso in cui un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato (se privo delle necessarie autorizzazioni) si introduca fraudolentemente presso la sede di un concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche

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

Tale fattispecie reato si realizza quando un soggetto "distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui". Tale reato è punito con la reclusione da sei mesi a tre anni

Il D.Lgs 7 del 15 gennaio 2016 recita: *"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."*

Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale

Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore

5.3.8 - 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.)

Tale reato si realizza quando un soggetto "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". Tale reato è punito con la reclusione da uno a quattro anni

La sanzione è da tre a otto anni se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

Il Dlgs 7 del 15 gennaio 2016 recita: "*la pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema*"

Questo delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica

Perché il reato si integri è sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato

5.3.9 - Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

Questo reato si realizza quando un soggetto "mediante le condotte di cui all'art. 635-bis (danneggiamento di dati, informazioni e programmi informatici), 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". Tale reato è punito con la reclusione da uno a cinque anni

Il Dlgs 7 del 15 gennaio 2016 recita: "*la pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema*"

Si tenga conto che qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di

danneggiamento dei dati previsto dall'art. 635-bis

Il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un virus)

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

Questo reato si configura quando "il fatto di cui all'art. 635-quater (Danneggiamento di sistemi informatici o telematici) 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". Tale reato è punito con la pena della reclusione da uno a quattro anni

La sanzione è della reclusione da tre a otto anni se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se lo stesso è reso, in tutto o in parte, inservibile

Il Dlgs 7 del 15 gennaio 2016 recita: "*la pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema*"

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità (art. 635-ter), quel che rileva è che il sistema sia utilizzato per il perseguimento di pubblica utilità indipendentemente dalla proprietà privata o pubblica del sistema stesso

Il reato si può configurare nel caso in cui un dipendente cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero che l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

5.3.11 - Frode informatica (art.640-ter c.p. modificato dal D.Lgs n. 36 del 10 aprile 2018)

Questo reato si configura quando chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno

La pena prevista è la reclusione da sei mesi a tre anni e la multa da € 51 a €1.032

La pena va da uno a cinque anni e la multa da €309 a €1.549 se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema

Se poi il fatto è commesso con furto e indebito utilizzo in danno di qualcuno la reclusione va da due a sei anni e la multa da €600 a € 3.000.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o taluna delle circostanze previste dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età', e numero

5.3.12 - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art.640-quinquies c.p.)

Questo reato si configura quando "il soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato". Tale reato è punito con la reclusione fino a tre anni e con la multa da Euro 51 a Euro 1.032

Questo reato può essere integrato da parte dei certificatori qualificati o meglio i soggetti che prestano servizi di certificazione di firma elettronica qualificata

5.4 - Le attività sensibili relative ai reati informatici

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 della società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto

L'analisi dei processi ha consentito di individuare le seguenti "attività sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24 - bis del d.lgs. 231/2001:

a. Gestione dei profili utente e del processo di autenticazione
b. Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici
c. Gestione e protezione della postazione di lavoro
d. Gestione degli accessi da e verso l'esterno
e. Gestione e protezione delle reti
f. Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD)
g. Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.)

I delitti trovano come presupposto l'utilizzo della rete informatica intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e precisamente:

- Tutte le attività aziendali svolte dal personale tramite l'utilizzo della rete aziendale, del servizio di posta elettronica e accesso ad Internet
- Gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica e applicativa IT nonché la sicurezza informatica
- Erogazione di servizi di installazione e servizi professionali di supporto al personale ed ai clienti (ad esempio,

assistenza, manutenzione, gestione della rete, manutenzione e security)

5.5 - Organi e funzioni aziendali coinvolte

In relazione alle descritte Attività Sensibili – tutte astrattamente ipotizzabili – si ritengono particolarmente coinvolti tutti gli organi e funzioni aziendali.

5.6 - Principi e regole di comportamento

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nel Modello e nella presente parte speciale del Modello

In generale, il sistema di organizzazione, gestione e controllo della società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, gli Amministratori, gli Organi Sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, devono conoscere e rispettare:

1. gli standard generali di controllo
2. i principi di comportamento individuati nel Codice Etico
3. quanto regolamentato dalla documentazione e dagli atti aziendali
4. le disposizioni di legge

5.7 -Principi e norme generali di comportamento

La presente Parte Speciale è inerente alle condotte poste in essere dai soggetti destinatari del Modello che operano, in particolare, nelle aree a Rischio reato informatico e nello svolgimento delle attività sensibili precedentemente citate

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Parte Speciale, in linea generale ed al fine di perseguire la prevenzione dei Reati Informatici è fatto espresso divieto a tutti i Soggetti coinvolti di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 24-bis del D. Lgs. 231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Parte Speciale

In generale, la prevenzione dei crimini informatici è svolta attraverso adeguate misure tecnologiche, organizzative e

normative ed in particolare almeno attraverso l'applicazione dei seguenti controlli di carattere generale:

- Previsione nel Codice Etico di specifiche indicazioni volte a impedire la commissione dei reati informatici sia all'interno della società che tramite apparecchiature non soggette al controllo della stessa
- Previsione di un idoneo sistema di sanzioni disciplinari (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del Modello) che violino in maniera intenzionale i sistemi di controllo o le indicazioni comportamentali fornite
- Predisposizione di adeguati strumenti tecnologici atti a prevenire e/o impedire la realizzazione di reati informatici da parte dei dipendenti e in particolare di quelli appartenenti alle strutture della società ritenute più esposte al rischio
- Predisposizione di programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle rstrse informatiche aziendali
- Azioni di adeguamento della struttura societaria alle disposizioni in materia di tutela dei dati personali previste dal Regolamento UE 2016/679 e dal D.lgs. 196/2003
- Adozione di Disciplinare interno aziendale per l'utilizzo delle risorse informatiche

Conseguentemente, gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nello svolgimento delle attività a rischio hanno l'espresso obbligo di perseguire i seguenti principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi di controllo specifici:

- **Segregazione delle attività**
  si richiede l'applicazione del principio di separazione delle attività e dei ruoli che intervengono nelle attività chiave dei processi operativi esposti a rischio, tra chi autorizza, chi esegue e chi controlla; in particolare, deve sussistere separazione dei ruoli di gestione di un processo e di controllo dello stesso; ad esempio: progettazione ed esercizio, acquisto di beni e risorse e relativa contabilizzazione
- **Esistenza di procedure**
  devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili. Le procedure devono definire formalmente le responsabilità e i ruoli all'interno del processo e le disposizioni operative e relativi controlli posti a presidio nelle attività
- **Poteri autorizzativi e di firma**
  definire livelli autorizzativi da associarsi alle attività critiche dei processi operativi esposti a rischio
- **Tracciabilità**
  tracciabilità degli accessi e delle attività svolte sui sistemi informatici che supportano i processi esposti a rischio; ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione distruzione delle registrazioni effettuate
- **Gestione delle segnalazioni**
  raccolta, analisi e gestione delle segnalazioni di fattispecie a rischio per i reati informatici rilevati da soggetti interni e esterni all'ente

- **Riporto all'OdV**
  riferire prontamente all'OdV eventuali situazioni di irregolarità

5.8 - Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.), gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nelle svolgimento delle attività a rischio sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'art. 24-bis del D.Lgs. 231/01, al rispetto delle regole e procedure aziendali emesse a regolamentazione di tale attività a rischio

Tali regole e procedure prevedono controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area quali, ad esempio:

- **Esistenza di una normativa/procedura aziendale relativa a:**
  1. Gestione degli accessi che tra l'altro individua le seguenti fasi:
     - Attribuzione accessi
     - Assegnazione dei codici identificativi personali (richieste di abilitazione/modifica delle utenze)
     - Disattivazione dei codici utente associati al personale che ha perso il diritto di accesso a tutti i sistemi informatici o che non accede più ai vari sistemi
     - Attività di controllo volta a verificare, prima della creazione di un'utenza, che la stessa non sia già stata precedentemente assegnata/disabilitata/rimossa e che uno stesso codice identificativo personale non venga assegnato, neppure in tempi diversi, a persone diverse
  2. Modalità di utilizzo e di salvaguardia del PC intese come misure che l'utente deve adottare per garantire un'adeguata Protezione delle apparecchiature incustodite
  3. Installazione di software sui sistemi operativi
  4. Dismissione dei supporti di memorizzazione su cui sono registrate informazioni aziendali

- **Attuazione di un sistema di accesso logico idoneo a controllare che le attività di utilizzo delle risorse da parte dei processi e degli utenti e di accesso alla rete si esplichino attraverso la verifica e la gestione dei diritti d'accesso**
- **Presenza di sistemi di protezione antivirus e antispam**
- **Esistenza di una serie di procedure, in materia di protezione dei dati personali, che disciplinano gli aspetti legati al corretto utilizzo delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni**
- **Attuazione del progetto di formazione, volta a sensibilizzare tutti gli utenti e/o particolari figure professionali, con l'obiettivo di diffondere all'interno della società le politiche, gli obiettivi e i piani previsti in materia di sicurezza informatica e al fine di soddisfare i requisiti previsti in materia di privacy**
- **Consegna a ciascun dipendente della Società, contestualmente all'assegnazione del pc e/o dell'indirizzo di posta internet di norme per l'utilizzo dei Personal Computer aziendali e sull'utilizzo della posta internet e in generale di documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico**

- **Individuazione tempestiva delle vulnerabilità dei sistemi**
- **Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse tecnologiche e informazioni), attraverso, l'adozione di sistemi antincendio, antiallagamento, di condizionamento, gruppi di continuità UPS e di regolamentazione degli accessi**
- **Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici (registrazione dei log on e log off)**
- **Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di networking attraverso tra l'altro una serie di provvedimenti volti a garantire che:**
  - L'informazione inserita e elaborata dal sistema pubblico sia processata completamente e in modo tempestivo
  - Le informazioni sensibili siano protette durante i processi di raccolta e di conservazione
  - L'accesso al sistema pubblico non consenta ingressi fortuiti alle reti con cui è connesso

Principi procedurali specifici

In particolare, si elencano qui di seguito le regole, le quali sono parte integrante del Disciplinare sull'uso di internet e sistemi informatici adottato dall'Azienda, che devono essere rispettate dalla società e dai dipendenti e dagli altri soggetti eventualmente autorizzati nell'ambito delle Attività Sensibili

- i dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come riservati
- è vietato introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del soggetto responsabile individuato
- è vietato in qualunque modo modificare la configurazione di postazioni di lavoro fisse o mobili effettuata dal Servizio Infrastrutture
- è vietato acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.)
- è vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla società
- è vietato divulgare, cedere o condividere con personale interno o esterno all'azienda le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti
- è vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti
- è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi
- è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi
- è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei

propri compiti lavorativi

- è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi
- è vietato comunicare a persone non autorizzate, interne o esterne alla società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati
- è proibito distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati
- è vietato lo spamming come pure ogni azione di risposta allo spam
- è obbligatorio segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

L'azienda si impegna a porre in essere i seguenti adempimenti:

- informare adeguatamente i dipendenti e gli altri soggetti eventualmente autorizzati dell'importanza di mantenere i propri codici di accesso (username e password) confidenziali e di non divulgare gli stessi a soggetti terzi (cfr. Manuale utilizzo User ID e password)
- fare sottoscrivere ai dipendenti e agli altri soggetti eventualmente autorizzati uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche aziendali
- informare i dipendenti e agli altri soggetti eventualmente autorizzati della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccare l'accesso al pc "lock computer", qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso (cfr. Manuale utilizzo User ID e password)
- impostare i sistemi informatici in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente
- fornire un accesso da e verso l'esterno (connessione alla rete Internet) esclusivamente ai sistemi informatici dei dipendenti o di eventuali soggetti terzi che ne abbiano la necessità ai fini lavorativi o connessi all'amministrazione societaria
- limitare gli accessi alla stanza server unicamente al personale autorizzato
- proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle
- fornire ogni sistema informatico di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati
- impedire l'installazione e l'utilizzo di software non approvati dalla società e non correlati con l'attività espletata per la stessa
- limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "virus") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e file)
- impedire l'installazione e l'utilizzo, sui sistemi informatici della società, di software (c.d. "P2P", di files sharing o di instant messaging) mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, virus, ecc.) senza alcuna possibilità di controllo da parte della società

- qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna WiFi), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni all'azienda, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti
- prevedere un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti e degli altri soggetti eventualmente autorizzati (es. Regole aziendali)
- limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei dipendenti e degli altri soggetti eventualmente autorizzati (i.e. connessione tramite VPN)
- effettuare periodicamente, in presenza di accordi sindacali che autorizzino in tale senso e ove possibile, controlli ex ante ed ex post sulle attività effettuate dal personale sulle reti nonché, quando verrà completato il progetto di anomaly detection, rielaborare con regolare cadenza i log dei dati al fine di evidenziare eventuali comportamenti anomali

5.9 - I controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'art. 24-bis del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'art. 24-bis del Decreto sono i seguenti:

- Svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'art. 24-bis del Decreto; con riferimento a tale punto, l'OdV condurrà controlli a campione sulle attività potenzialmente a rischio di delitti informatici, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere
- Proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei delitti informatici di cui alla presente Parte Speciale, anche in considerazione del progresso e dell'evoluzione delle tecnologie informatiche

- Proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Parte Speciale
- Monitorare il rispetto delle procedure e la documentazione interna (i.e. Normativa Aziendale e Modulistica) per la prevenzione dei Delitti Informatici in costante coordinamento con le funzioni Sicurezza Informatica ed Internal Audit
- Consultarsi con il responsabile della Sicurezza Informatica e/o del Servizio Sistemi Informativi ed invitare

periodicamente lo stesso a relazionare alle riunioni dell'OdV

- Esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute
- Conservare traccia dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante

Organizzazione

Digitronica.IT S.p.A.

Sede: Viale del Lavoro, 52 Verona
Phone: 045 50 19 01
Fax: 045 50 22 58
Email: info@digitronica.it
Pec: digitronica.it@pec.it

MOGC 231 – PARTE SPECIALE

ai sensi del D.Lgs.n.**231** del 8 Giugno 2001 e s.m.i.

Master	☐
Copia controllata	☐
Copia non controllata	☐
Numero della copia	☐

Emissione DG	Data		Firma	
Approvazione DG	Data		Firma	
Approvazione ODV	Data		Firma	

Stato delle revisioni

Versione	Data	Descrizione	Autore
00	*04/06/2019*	Prima emissione	Digitronica.IT Srl
01	*01/12/2020*	Aggiornamento	Digitronica.IT S.p.A.
02	*01/04/2022*	Aggiornamento	Digitronica.IT S.p.A.
03	*22/01/2024*	Aggiornamento OdV	Digitronica.IT SpA

Indice generale della sezione

Modello di Organizzazione, Gestione e Controllo – Parte speciale

6.1 Introduzione e funzione della parte speciale di reati tributari

La presente parte speciale si riferisce ai reati tributari di cui all'Art. 25-quinquiesdecies del D.Lgs.n.231/2001 ed ha come obiettivo che tutti i destinatari, ossia amministratori, dirigenti e dipendenti aziendali nonché consulenti e collaboratori, adottino regole di condotta conformi a quanto prescritto dal D.Lgs.n.231/2001 al fine di prevenire il verificarsi dei reati sopra richiamati.

In particolare, la presente Parte Speciale ha lo scopo di:

- fornire le regole di comportamento e le procedure che gli amministratori, i dirigenti ed i dipendenti, nonché i consulenti, liberi professionisti e partner aziendali sono tenuti ad osservare ai fini della corretta applicazione del Modello
- fornire all'Organismo di Vigilanza ed ai responsabili delle altre funzioni aziendali che cooperano con il medesimo, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

6.2 Le fattispecie di reato richiamate dal D.Lgs.n.231/2001

Con l'entrata in vigore del **Decreto Legge 26 ottobre 2019, n. 124**, i cosiddetti *"reati tributari"* - disciplinati dal Decreto Legislativo 10 marzo 2000, n. 74 - entrano a far parte dei *"reati presupposto"* previsti dal D. Lgs. 231/2001.

Invero, per effetto dell'introduzione del citato Decreto Legge, soltanto il delitto di dichiarazione fraudolenta mediante utilizzo di fatture o altra documentazione per operazioni inesistenti *ex* art. 2 D. Lgs. 74/2000 costituiva una fattispecie criminosa idonea ad ingenerare la responsabilità amministrativa dell'ente. Di contro, in sede di conversione (avvenuta con la **Legge 19 dicembre 2019, n. 157**), i reati tributari contemplati dal nuovo articolo 25-quinquiesdecies D. Lgs. 231/01 sono:

1) il delitto di **dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** (art. 2, comma I e II-bis, D. Lgs. 74/2000);
2) il delitto di **dichiarazione fraudolenta mediante altri artifici** (art. 3 D. Lgs. 74/2000);
3) il delitto di **emissione di fatture o altri documenti per operazioni inesistenti** (art. 8, comma I e II-bis, D. Lgs. 74/2000);
4) il delitto di **occultamento o distruzione di documenti contabili** (art. 10 D. Lgs. 74/2000);
5) il delitto di **sottrazione fraudolenta al pagamento di imposte** (art. 11 D. Lgs. 74/2000).

Trattasi di fattispecie la cui integrazione determina l'applicazione sia di sanzioni pecuniarie sia di sanzioni interdittive (quelle di cui alle lettere c), d) ed e) dell'art. 9 D. Lgs. 231/2001: il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi).

Non determinava, invece, responsabilità amministrativa in capo all'ente la commissione di altri reati tributari, quali, ad esempio, i delitti di dichiarazione infedele (art. 4 D. Lgs. 74/2000), di omessa dichiarazione (art. 5 D. Lgs. 74/2000), di omesso versamento (artt. 10-bis e 10-ter D. Lgs. 74/2000) e di omesso versamento mediante indebita compensazione (art. 10-quater D. Lgs. 74/2000).

Nondimeno, a seguito dell'entrata in vigore del **Decreto Legislativo 14 luglio 2020, n. 75** (*"Attuazione della direttiva /UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale"*), avvenuta il 30 luglio 2020, è stata novellata - oltre al resto - la disposizione di cui all'art. 25-quinquiesdecies D. Lgs. 231/01.

In conformità a quanto stabilito dalla Direttiva PIF, l'intervento normativo ha riguardato il testo del Decreto Legislativo 213/01, modificato attraverso un sensibile ampliamento della responsabilità amministrativa degli enti in relazione a nuove figure di reato presupposto.

In particolare, è stato inserito dall'art. 5, comma 1, lett. c), D. Lgs. 75/2020, un nuovo comma 1-bis nell'art. 25-quinquiesdecies D. Lgs. 231/01, che recita:

"In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro".

I reati presupposto inseriti dal D.Lgs.n.75 del 14 luglio 2020 sono:

- **Dichiarazione infedele -Art.4 D.Lgs.n.74/2000**
- **Omessa dichiarazione -Art.5 D.Lgs.n.74/2000**
- **Indebita compensazione - Art.10-quater D.Lgs.n.74/2000**

Merita, infine, aggiungere che il D. Lgs. 75/2020 ha introdotto una deroga al principio di cui all'art. 6 D.Lgs. 74/2000 in virtù del quale la forma di manifestazione del "tentativo" non si configura in relazione alla commissione delle fattispecie penali tributarie previste dagli articoli 2, 3 e 4 del testo normativo in esame ("I delitti previsti dagli articoli 2, 3 e 4 non sono comunque punibili a titolo di tentativo").

L'azienda è sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali.
A tal fine, ha avviato un progetto di analisi dei propri strumenti organizzativi, di gestione e di controllo, in considerazione dei reati previsti dall' Art. 25-quinquiesdecies del Decreto Legislativo 231/01, volto a verificare la rispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto

In considerazione delle caratteristiche societarie ed organizzative di Digitronica.IT, la presente Parte Speciale riguarda i seguenti reati previsti dall'art.25-quinquiesdecies del D.Lgs.n.231/01:
1) il delitto di **dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** (art. 2, comma I e II-bis, D. Lgs. 74/2000);
2) il delitto di **dichiarazione fraudolenta mediante altri artifici** (art. 3 D. Lgs. 74/2000);
3) il delitto di **emissione di fatture o altri documenti per operazioni inesistenti** (art. 8, comma I e II-bis, D. Lgs. 74/2000);
4) il delitto di **occultamento o distruzione di documenti contabili** (art. 10 D. Lgs. 74/2000);
5) il delitto di **sottrazione fraudolenta al pagamento di imposte** (art. 11 D. Lgs. 74/2000).

6.3.1 Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art. 2 D.Lgs.n.74 modificato da Art. 39 del D.L. n.124 del 26 ottobre 2019)

L'Art.2 punisce chi al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.

Si riporta il testo dell'Art. 2 del D.L.gs 74 modificato al comma 1, con l'aggiunta del comma 2-bis.

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.

2. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

2-bis. Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dal comma 1, la sanzione pecuniaria fino a cinquecento quote.

Per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dal comma 2-bis, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

6.3.2 Dichiarazione fraudolenta mediante altri artifici (Art. 3 D.Lgs.n.74 modificato da Art. 39 del D.L. n.124 del 26 ottobre 2019)

L'Art.3 punisce chi al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti tende ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria.

Si riporta il testo dell'Art. 3 del D.L.gs.n.74 modificato al comma 1

1. Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:

- L'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila
- L'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo

dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

2. Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

3. Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

Per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote.
Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

6.3.3 Dichiarazione infedele (Art. 4 D.Lgs.n.74 modificato da Art. 39 del D.L. n.124 del 26 ottobre 2019 e inserito da D.Lgs.n.75 del 14 luglio 2020)

L'Art.4 punisce chi al fine di evadere le imposte sui redditi o sul valore aggiunto, indica nella dichiarazione annuale elementi attivi o passivi diversi o inesistenti.

Si riporta il testo dell'Art. 4 del D.L.gs.n.74

1. Fuori dei casi previsti dagli articoli 2 e 3, è punito con la reclusione da due anni a quattro anni e sei mesi chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:
a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila
b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni
1-bis. Ai fini dell'applicazione della disposizione del comma 1, non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali.
1-ter. Fuori dei casi di cui al comma 1-bis, non danno luogo a fatti punibili le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette. Degli importi compresi in tale percentuale non si tiene conto nella verifica del superamento delle soglie di punibilità previste dal comma 1, lettere a) e b).

Per il delitto di dichiarazione infedele, previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote.
Se, in seguito alla commissione dei delitti indicati al comma 1 e 1-bis, l'ente ha conseguito un profitto di rilevante

entità, la sanzione pecuniaria è aumentata di un terzo.

6.3.4 Omessa dichiarazione (Art. 5 D.Lgs.n.74 modificato da Art. 39 del D.L. n.124 del 26 ottobre 2019 e inserito da D.Lgs.n.75 del 14 luglio 2020)

L'Art.5 punisce il soggetto obbligato o il sostituto di imposta che, al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta una delle dichiarazioni relative a dette imposte

Si riporta il testo dell'Art. 5 del D.L.gs.n.74

1. È punito con la reclusione da due a cinque anni chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila.
1-bis. È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.
2. Ai fini della disposizione prevista dai commi 1 e 1-bis non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto.

Per il delitto di omessa dichiarazione, previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote.
Se, in seguito alla commissione dei delitti indicati al comma 1 e 1-bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

6.3.5 Emissione di fatture o altri documenti per operazioni inesistenti (Art.8 D.Lgs.n.74 modificato da Art. 39 del D.L. n.124 del 26 ottobre 2019)

L'Art.8 punisce chi emette fatture inesistenti per consentire evasione a terzi di imposte sui redditi o sul valore aggiunto

Si riporta il testo dell'Art. 8 del D.L.gs.n.74 modificato al comma 1 e con l'aggiunta del comma 2-bis

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

2. Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

2-bis. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote
Per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la

sanzione pecuniaria fino a quattrocento quote

Se, in seguito alla commissione dei delitti indicati al comma 1 e 1-bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

6.3.6 Occultamento o distruzione di documenti contabili (Art.10 D.Lgs.n.74 modificato da Art. 39 del D.L. n.124 del 26 ottobre 2019)

L'Art.10 punisce chi distrugge o occulta documentazione per evadere o far evadere imposte sui redditi o sul valore aggiunto

Si riporta il testo dell'Art. 10 del D.L.gs 74 modificato al comma 1

1. Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

6.3.7 Indebita compensazione (Art. 10-quater D.Lgs.n.74 inserito da D.Lgs.n.75 del 14 luglio 2020)

L'Art.10-quater punisce chi vantando crediti non spettanti, li utilizza in compensazione su somme dovute

Si riporta il testo dell'Art. 10-quater del D.L.gs.n.74

1. È punito con la reclusione da sei mesi a due anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro.
2. È punito con la reclusione da un anno e sei mesi a sei anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro.

Per il delitto di indebita compensazione, previsto dall'articolo 10-quater, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1 e 2, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

6.3.8 Sottrazione fraudolenta al pagamento di imposte(Art.11 D.Lgs.n.74)

L'Art.11 punisce chi, per non pagare imposte sui redditi o sul valore aggiunto o altro, si adopera per rendere inefficace la procedura di riscossione

Si riporta il testo dell'Art. 11 del D.L.gs.n.74 e s.m.i.

1. Salvo che il fatto costituisca più grave reato è punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.
2. Salvo che il fatto costituisca più grave reato è punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

Per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1 e 2, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

6.4 Le attività sensibili relative ai reati tributari

L'Art. 6, comma 2, lettera a) del D.Lgs.n.231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal decreto, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs.n.231/2001

L'analisi svolta nel corso del Progetto ha permesso di individuare le attività della Società che potrebbero essere considerate "sensibili" con riferimento al rischio di commissione dei reati richiamati dall'**Art. 25-quinquiesdecies** del D.Lgs.n.231/2001.

Le aree a rischio "diretto" coprono l'intera area amministrativa-contabile della Società, in modo particolare quelle interessate alle operazioni in materia di imposte e di versamenti di IVA, ed in particolare si ritiene debbano rientrare tra le attività a rischio:

1) Gestione anagrafica clienti e fornitori
2) Emissione delle fatture attive.

3) Registrazione delle fatture e delle note di credito.
4) Credit management.
5) Archiviazione della documentazione a supporto delle fatture emesse.
6) Registrazioni di carico e scarico merci da magazzino
7) Cessione di immobili aziendali o partecipazioni.
8) Operazioni straordinarie.
9) Disposizioni dai conti correnti bancari.
10) Gestione del sistema di qualificazione dei fornitori.
11) Raccolta e controllo delle richieste di acquisto.
12) Richieste di offerte/preventivi, valutazione delle offerte, selezione dei fornitori e negoziazione.
13) Emissione degli ordini di acquisto e stipulazione dei contratti.
14) Gestione dei trasporti di materie prime/ semilavorati/ prodotti finiti.
15) Gestione degli acquisti urgenti e gestione dei conferimenti di incarichi a consulenti / professionisti esterni. Verifica delle prestazioni/beni acquistati.
16) Liquidazione delle fatture.
17) Monitoraggio delle fatture da ricevere e in scadenza.
18) Gestione delle attività di contabilizzazione degli acconti pagati ai fornitori.
19) Fatturazione elettronica.
20) Back up con strumenti informatici dell'archivio contabile.
21) Effettuazione del calcolo delle imposte dirette e indirette, esecuzione dei versamenti relativi, predisposizione e trasmissione delle relative dichiarazioni.
22) Attività che prevedono una interazione diretta con l'Amministrazione finanziaria (svolgimento di verifiche tributarie, presentazione di interpelli, avvio di contenzioso tributario, ecc.).
23) Gestione delle spese di rappresentanza sostenute.
24) Gestione della tesoreria.

6.5 Organi e funzioni aziendali coinvolte

In relazione ai reati e alle condotte criminose ed alle attività sensibili sopra esplicitate, le funzioni aziendali ritenute più specificamente a rischio risultano essere, anche in riferimento alle attività svolte dall'azienda le seguenti:

- Finanza e Amministrazione
- Acquisti, Logistica e Ufficio Commerciale
- Direzione Aziendale

Eventuali integrazioni delle suddette Aree a Rischio potranno essere disposte dal Presidente del Consiglio di Amministrazione, anche su indicazione dell'Organismo di Vigilanza, al quale viene dato mandato di individuare le relative ipotesi e di definire gli opportuni provvedimenti operativi.

6.6 Principi e regole di comportamento

Tutte le Attività Sensibili devono essere svolte conformandosi alle leggi vigenti, nonché alle procedure aziendali, ai valori e alle regole contenute nel Modello e nel Codice Etico.

In linea generale, il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli, in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

6.7 Principi e norme generali di comportamento

La presente Parte Speciale prevede **l'espresso divieto** a carico degli Organi Sociali aziendali, dei Dipendenti/Collaboratori, e Consulenti/Partner nella misura necessaria alle funzioni dagli stessi svolte, di:

- porre in essere, promuovere, collaborare o dare causa alla realizzazione di comportamenti tali che integrino, direttamente o indirettamente, le fattispecie che configurano i cosiddetti *"reati tributari"*;
- utilizzare, anche in via meramente occasionale, l'impresa, o una sua unità organizzativa, allo scopo di consentire o agevolare la commissione dei reati di cui sopra;
- fornire, direttamente o indirettamente, specie attraverso l'emissione di fatture, assistenza a soggetti che intendano porre in essere i predetti reati;
- avvalersi di professionisti che offrono prestazioni illecite, che configurano un concorso nella commissione di uno o più reati tributari;
- compiere operazioni finanziarie e predisporre documenti contabili anomali per tipologia o oggetto e instaurare o mantenere rapporti che presentino profili di anomalia dal punto di vista dell'affidabilità e reputazione dei soggetti;
- distruggere documenti contabili.

6.8 Procedure specifiche per aree sensibili

La presente Parte Speciale prevede le seguenti procedure specifiche per le Attività Sensibili, come individuate al precedente paragrafo 6.4:

- qualunque transazione finanziaria deve presupporre **la conoscenza del beneficiario della relativa somma**;
- le **operazioni di rilevante entità** devono essere concluse con persone fisiche e giuridiche verso le quali siano state preventivamente svolte **idonee verifiche, controlli e accertamenti**;
- nel caso in cui alla società venga proposta una **operazione anomala**, essa viene sospesa e valutata preventivamente dal Presidente del CdA il quale valuta la comunicazione all'OdV.: quest'ultimo esprimerà il proprio parere sull'opportunità dell'operazione e provvederà eventualmente a stabilire le cautele necessarie, da adottare per il proseguimento della stessa, nonché a rendere in merito un parere, del quale dovrà tenersi conto in sede di approvazione e svolgimento dell'operazione stessa;
- deve essere **delegato preventivamente** un soggetto avente la funzione di **eseguire i pagamenti** verso soggetti esterni e di **valutare le fatture ricevute** dall'impresa, nonché di chiedere periodicamente **informazioni al professionista esterno** incaricato dell'assolvimento degli incombenti fiscali;

- **i dati raccolti**, relativamente ai rapporti con clienti e collaboratori esterni, devono essere **completi, aggiornati ed archiviati,** sia per la corretta e tempestiva individuazione dei soggetti, che per una valida valutazione del loro profilo;
- ogni **mutamento in merito al nominativo del professionista** incaricato dell'assolvimento degli incombenti fiscali dovrà essere **comunicato all'OdV**;
- deve essere mantenuto un **rapporto di collaborazione con l'Amministrazione finanziaria**;
- qualunque **attività ispettiva e/o di accertamento** compiuta dagli Organi dell'Amministrazione finanziaria deve essere tempestivamente **comunicata all'OdV**;
- **l'inosservanza dei termini stabiliti** per la presentazione delle dichiarazioni deve essere tempestivamente **comunicata all'OdV**;
- per i **flussi monetari e/o finanziari in entrata ed in uscita** seguire la procedura interna sulla Finanza Dispositiva **(P-INT 01 Finanza Dispositiva);**
- seguire la procedura interna relativa alla **Formazione del bilancio civilistico (P-INT 02 Formazione del Bilancio Civilistico);**
- **l'inserimento anagrafico di nuovi clienti e la variazione dei dati presenti** sono specificatamente attribuiti unicamente alla Responsabile della funzione Finanza e Amministrazione e ad un suo collaboratore, attraverso **l'attribuzione di specifico profilo autorizzato** a compiere dette operazione sul gestionale aziendale. Di dette operazioni sono mantenuti i file di log per un periodo ritenuto congruo;
- deve essere effettuato il **back up giornaliero incrementale e settimanale totale dei server** contenenti documenti fiscali e devono essere previste **restrizioni all'accesso ai backup** stessi che è consentito solo agli Amministratori di Sistema, formalmente nominati;
- **monitoraggio costante**, attraverso uno scadenzario, degli **adempimenti di legge**, al fine di evitare ritardi e imprecisioni nella presentazione di dichiarazioni e/o documenti fiscali;
- **controllo trimestrale formalizzato**, da parte del Collegio Sindacale, di completezza ed accuratezza delle **imposte pagate e sui crediti maturati** nei confronti dell'erario;
- le **trasferte dei dipendenti** della durata superiore alle 24 ore sono previamente autorizzate dal Presidente del CdA;
- le trasferte effettuate in macchina sono rimborsate sulla base delle **tabelle chilometriche** ufficiali dell'Automobile Club Italia;
- **monitoraggio su rimborsi per trasferte eccessivi** rispetto alla norma e **segnalazione al Presidente del CdA** che, qualora lo ritenga rilevante, ne **informerà l'OdV**;
- deve essere chiaramente individuato, attraverso specifica **delega**, il **responsabile della gestione della tesoreria**;
- devono essere effettuate **verifiche** in ordine all'effettuazione di **pagamenti in Paesi a fiscalità privilegiata** ed in caso sospendere il pagamento ed **informarne immediatamente il Presidente del CdA e l'OdV**;
- deve essere sempre **verificata la correttezza dei dati inseriti** nella richiesta di pagamento e successiva contabilizzazione;
- **divieto di richiedere anticipi in contanti** o di ritirare contanti con le carte di credito aziendali:

- per i **beni materiali** ogni **persona incaricata nel processo di vendita verifica** -in base alla propria responsabilità ed attraverso l'inserimento nel sistema gestionale- la coerenza tra: ordine di vendita accettato, contratto, movimentazione di scarico merce da magazzino, documento di trasporto, fattura attiva, incasso del credito;
- per i **servizi** ogni **persona incaricata nel processo di vendita verifica** -in base alla propria responsabilità ed attraverso l'inserimento nel sistema gestionale- la coerenza tra: contratto di prestazione del servizio, fattura attiva, incasso del credito, nonché la raccolta di documentazione della effettività del servizio reso;
- i **prezzi di vendita** devono essere indicati chiaramente nelle **offerte commerciali**, chiunque rilevi uno scostamento dalle condizioni pattuite e/o dalle normali condizioni di mercato ne informa immediatamente la Direzione;
- nello **statuto societario** è presente il disegno di una governance societaria che prevede **adeguati livelli decisionali** (ad es. la delibera da parte del consiglio di amministrazione), per **operazioni di straordinaria amministrazione**, quali la compravendita di beni immobili e partecipazioni societarie;
- devono essere seguite le **procedure per la gestione degli acquisti** individuate nel Manuale Integrato del SGI ISO 9001 ed ISO 27001 adottato da Digitronica.IT;
- devono essere seguiti i **criteri di selezione del fornitore** adottati dalla Società, ovvero richiesta di DURC e CIA alla prima fornitura, ed inserimento nell'albo fornitori aziendale dopo tre forniture andate a buon fine;
- devono essere indicati nel gestionale le **valutazioni effettuate** e le **decisioni prese relativamente alla valutazione delle offerte dei fornitori**, indicando chiaramente chi ha preso la decisione, quando e per quali motivi;
- nella fase di **liquidazione delle fatture** deve sempre esserci un controllo al fine di verificare la **corrispondenza tra la denominazione/ragione sociale del fornitore e l'intestazione del conto corrente**;
- gli **accordi con i fornitori** devono essere **formalizzati** attraverso apposito contratto o accordo di partnership con relative lettere di attivazione;
- devono essere inserite, negli accordi contrattuali, **clausole di rispetto del codice etico aziendale del Modello organizzativo** ex D.Lgs. n. 231/2001, con sanzioni che possono comportare la risoluzione del rapporto contrattuale;
- attraverso il sistema gestionale aziendale deve avvenire il **monitoraggio degli ordini aperti** al fine di evitare il rischio di registrazione di transazioni improprie;
- controllo, attraverso i sistemi informatici aziendali, al fine di **evitare la duplice registrazione della fattura** e dei pagamenti;
- **segregazione delle funzioni aziendali** coinvolte nel processo, in particolare tra la gestione dell'ordine, la gestione dei pagamenti, l'autorizzazione degli stessi e la registrazione delle spese;
- **attestazione,** in forma scritta via e-mail, da parte del soggetto aziendale destinatario della prestazione (beni/servizi) della **corrispondenza** tra quanto **richiesto** e quanto effettivamente **ricevuto/erogato**;
- **non devono essere ammessi anticipi o rimborsi** delle spese sostenute direttamente dai **soggetti esterni** rappresentanti della Pubblica Amministrazione che beneficiano di ospitalità;
- la **gestione dei rimborsi** spese deve avvenire in accordo con la **normativa**, anche fiscale, applicabile;
- i processi di **autorizzazione e controllo delle trasferte** devono essere sempre ispirati a criteri di economicità e di massima trasparenza, sia nei confronti della regolamentazione aziendale interna che nei confronti delle leggi e

delle normative fiscali vigenti;

- **l'archiviazione dei documenti** contabili, le scritture contabili obbligatorie, i registri fiscali obbligatori deve avvenire seguendo le **disposizioni normative**;
- il sostenimento di **spese di rappresentanza** deve soddisfare il concetto di **"opportunità" della spesa**, in linea pertanto con gli obiettivi aziendali;
- copia delle **quietanze relative al pagamento delle imposte** deve essere **trasmessa all'OdV**

Si rinvia, altresì, alle azioni di miglioramento previste per i reati societari.

6.9 I controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui alla presente Parte Speciale, commessi nell'interesse o a vantaggio dell'azienda, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello

Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati tributari sono i seguenti:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati alla presente Parte Speciale;
- monitorare sul rispetto delle procedure per la prevenzione della commistione di reati tributari in costante coordinamento con le funzioni di direzione ed amministrazione del personale;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- potrà richiedere, in qualunque momento, tutta la documentazione contabile e fiscale in merito a una o più specifiche operazioni, nonché esaminare tutte le dichiarazioni presentate dall'ente all'Agenzia delle Entrate;
- potrà richiedere informazioni ai professionisti esterni incaricati di tenere la contabilità e di svolgere gli incombenti fiscali a cui l'ente è tenuto;
- potrà sottoporre la documentazione acquisita all'attenzione di professionisti di comprovata esperienza;
- potrà sollecitare il pagamento delle imposte, specie nelle ipotesi in cui sia ipotizzabile il superamento delle soglie di punibilità previste dalla disciplina contenuta nel Decreto Legislativo 74/2000.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Organizzazione

Digitronica.IT S.p.A.

Sede: Viale del Lavoro, 52 Verona
Phone: 045 50 19 01
Fax: 045 50 22 58
Email: info@digitronica.it
Pec: digitronica.it@pec.it

MOGC 231 – PARTE SPECIALE

ai sensi del D.Lgs.n.**231** del 8 Giugno 2001 e s.m.i.

Master	
Copia controllata	
Copia non controllata	
Numero della copia	

Emissione DG	Data		Firma	
Approvazione DG	Data		Firma	
Approvazione ODV	Data		Firma	

Stato delle revisioni

Versione	Data	Descrizione	Autore
00	*04/06/2019*	Prima emissione	**Digitronica.IT Srl**
01	*01/12/2020*	Aggiornamento	**Digitronica.IT S.p.A.**
02	*01/04/2022*	Aggiornamento	**Digitronica.IT S.p.A.**
03	*22/01/2024*	Aggiornamento OdV	**Digitronica.IT SpA**

Indice generale della sezione

Modello di Organizzazione, Gestione e Controllo – Parte speciale

7.1 Introduzione e funzione della parte speciale di reati contro la Pubblica Amministrazione

Nella presente Parte Speciale vengono esaminati i profili di rischio relativi ai reati presupposto che rientrano nella categoria dei reati contro la Pubblica Amministrazione, ovvero tutti i reati elencati negli articoli 24 e 25 del d.lgs. 231/2001.

Per affinità di bene giuridico tutelato, si è ritenuto opportuno considerare in questa Parte Speciale anche il reato di cui all'art. 377 *bis* del codice penale, "*Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*", previsto come reato presupposto della responsabilità dell'ente dall'art. 25 *decies* del d.lgs. 231/01.

7.2 Le fattispecie di reato richiamate dal D.Lgs.n.231/2001

La conoscenza della struttura e delle modalità realizzative delle fattispecie di reato, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D. Lgs. 231/2001 è collegato il regime di responsabilità a carico dell'Ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

Si riportano, pertanto, i riferimenti normativi e le descrizioni dei reati oggetto della presente Parte Speciale.

7.2.1 Reati di corruzione e concussione

Art. 317 c.p. Concussione
"Il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei a dodici anni".

Art. 318 c.p. Corruzione per l'esercizio della funzione
"Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da uno a sei anni".

Art. 319 c.p. Corruzione per un atto contrario ai doveri d'ufficio
"Il pubblico ufficiale, che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da sei a dieci anni".

Art. 319 - bis c.p. Circostanze aggravanti
"La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene".

Art. 319 – ter c.p. Corruzione in atti giudiziari
"Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale

o amministrativo, si applica la pena della reclusione da sei a dodici anni. Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da cinque a dodici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da otto a venti anni".

Art. 319 – quater c.p. Induzione indebita a dare o promettere utilità

"Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei anni a dieci anni e sei mesi. Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni".

Art. 320 c.p. Corruzione di persona incaricata di un pubblico servizio

"Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio. In ogni caso, le pene sono ridotte in misura non superiore ad un terzo".

Art. 321 c.p. Pene per il corruttore

"Le pene stabilite nel primo comma dell'articolo 318, nell'art. 319, nell'art.319 bis, e nell'art. 320 in relazione alle suddette ipotesi degli articoli 318 e 319 si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altra utilità".

Art. 322 c.p. Istigazione alla corruzione

"Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel comma 1 dell'articolo 318, ridotta di un terzo. Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo. La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri. La pena di cui al comma secondo si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319".

Art. 322-bis c.p. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri

"*Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:*

1. ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;

2. ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;

3. alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;

4. ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

5. a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio.
Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:
1. alle persone indicate nel primo comma del presente articolo;
2. a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica o finanziaria. Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi".

Brevi cenni sulle fattispecie

Per maggiore chiarezza, pare opportuno individuare i soggetti appartenenti alla Pubblica Amministrazione che sono indicati dal legislatore nelle fattispecie sopra elencate.
Le nozioni di Pubblico Ufficiale e di Incaricato di Pubblico Servizio sono definite dal codice penale rispettivamente agli articoli 357 e 358.
In entrambi i casi il legislatore offre una nozione sostanziale delle due figure ancorandole alle attività svolte in concreto e non a qualifiche meramente formali.
Infatti, è "Pubblico Ufficiale", ai sensi della legge penale, non solo colui che ha un rapporto organico all'interno della Pubblica Amministrazione ma, più in generale, il soggetto che esercita pubbliche funzioni e che, nell'ambito della potestà pubblica, esercita poteri autoritativi, deliberativi o certificativi.
E', invece, "Incaricato di Pubblico Servizio" colui che svolge attività oggettivamente diretta al conseguimento di finalità pubbliche, anche a prescindere da un eventuale rapporto di lavoro dipendente dalla P.A.
Ciò che distingue le due figure è che il primo esercita dei poteri propri della Pubblica Amministrazione, il secondo, invece, ne è privo.
Quanto alla nozione di Pubblica Amministrazione, è bene fare riferimento ad una definizione ampia, ritenendosi tale scelta maggiormente prudenziale. Pertanto, deve intendersi Pubblica Amministrazione, ai fini della legge penale, qualsiasi ente che esercita funzioni di natura pubblica imputabili allo Stato o ad altra Istituzione.
A titolo esemplificativo e non esaustivo si riporta di seguito un elenco dei soggetti con cui la Società può venire in contatto con maggiore frequenza e che rientrano nella definizione di Pubblica Amministrazione:
• Regioni, Province e Comuni;
• Magistratura, Forze Armate e di Polizia (Guardia di Finanza, ARPA, SPRESAL, ASL, NOE, etc.);
• Agenzia delle Entrate;
• Amministrazioni, aziende ed Enti del Servizio Sanitario Nazionale;
• Camera di commercio;
• INAIL - Istituto nazionale assicurazioni infortuni sul lavoro, INPS – Istituto nazionale della previdenza sociale;
• Imprese pubbliche e soggetti privati che adempiono una funzione di interesse pubblico.
Quanto alle condotte descritte dagli articoli sopra enunciati, occorre rilevare come il concetto giuridico di "corruzione" sia affine a quello comunemente inteso e consista nella promessa o dazione di denaro o altra utilità per il compimento di un atto proprio della sua funzione o di un atto contrario ai doveri d'ufficio del Pubblico Ufficiale o dell'Incaricato di Pubblico

Servizio. Tale reato può essere realizzato non solo prima ma anche dopo il compimento, da parte dei soggetti sopra indicati, di un atto contrario ai doveri d'ufficio o dell'atto lecito.
La concussione, invece, deve essere commentata unitamente alla fattispecie di cui all'art. 319 quater, posto che la loro differenza è piuttosto sottile. Infatti, se nella concussione il soggetto agente, appartenente alla P.A., "costringe" il privato cittadino a compiere un'azione non dovuta (dare o promettere denaro o utilità), così esercitando una violenza psichica che non rende punibile il cittadino che la subisce, l'induzione costituisce un sopruso indiretto e mediato cui il soggetto privato può non dar seguito e che, tuttavia, si attiva, comprendendo il messaggio e provvedendo a darvi corso, così determinandone la punibilità.

Si precisa, infine, che con l'entrata in vigore della Legge n. 69/15 del 27 maggio 2015, oltre ad alcune modifiche in relazione al trattamento sanzionatorio irrogabile, il legislatore ha introdotto all'art. 129, comma 3 delle norme di attuazione del codice di procedura penale di cui al decreto legislativo 28 luglio 1989, n. 271 la previsione di un flusso informativo verso l'Autorità nazionale anticorruzione, da parte del pubblico ministero che eserciti l'azione penale per i delitti di cui agli articoli 317, 318, 319, 319 bis, 319 ter, 319 quater, 320, 321, 322, 322 bis, 346 bis, 353 e 353 bis del codice penale.

7.2.2 Truffa aggravata ai danni dello Stato o di altro Ente Pubblico

Art. 640, comma 2, c.p. Truffa aggravata dall'essere stata commessa ai danni dello Stato o di altro Ente Pubblico
"Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare […]".

Art. 640 - bis c.p. Truffa aggravata per il conseguimento di erogazioni pubbliche
"La pena è della reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee".

Brevi cenni sulle fattispecie
Si tratta di fattispecie di reato che consistono, per quanto attiene alla condotta, nel modificare il vero in ordine a fatti o circostanze la cui esistenza, nei termini falsamente rappresentati, è essenziale per l'atto di disposizione patrimoniale della Pubblica Amministrazione.
Un esempio concreto di una fattispecie di truffa potrebbe riguardare, ad esempio, il caso in cui, nella predisposizione di documenti, dati o informazioni necessaria alla partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta) al fine di ottenere l'aggiudicazione della gara stessa.

7.2.3 Frode informatica

Art. 640 – ter c.p. Frode informatica

"Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da Euro 51 a 1.032. La pena è della reclusione da uno a cinque anni e della multa da Euro 309 a 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante".

Brevi cenni sulla fattispecie

Occorre preliminarmente osservare come tale fattispecie abbia rilievo ai fini della responsabilità della Società soltanto quando è commesso a danno della Pubblica Amministrazione come sopra intesa. Pertanto, il reato può essere integrato qualora si violi un sistema informatico e ne si alterino i dati al fine di ottenere un profitto: ad esempio, una volta ottenuto un finanziamento, si viola il sistema informatico dell'Amministrazione erogante al fine di inserire un importo relativo al finanziamento superiore a quello ottenuto legittimamente.

7.2.4 Reati in tema di erogazioni pubbliche

Art. 316 - bis c.p. Malversazione a danno dello Stato

"Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni".

Art. 316 - ter c.p. Indebita percezione di erogazioni a danno dello Stato

"Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. Quando la somma indebitamente percepita è pari o inferiore a Euro 3.999,96 si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da 5164 a 25.822 di Euro. Tale sanzione non può comunque superare il triplo del beneficio conseguito".

Brevi cenni sulle fattispecie

La prima delle due ipotesi di reato sopra riportata, ovvero la malversazione, si configura nel caso in cui, avendo ottenuto da parte di un Ente Statale o dell'Unione Europea contributi, sovvenzioni o finanziamenti, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate. Il reato sussiste anche se la somma viene distratta solo parzialmente,

non rilevando il fatto che l'attività programmata si sia comunque svolta.
Il secondo reato, invece, si realizza nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere ovvero mediante l'omissione di informazioni dovute - si ottengano contributi, finanziamenti, mutui agevolati o altre erogazioni. In questo caso, contrariamente a quanto visto al punto precedente (art. 316-bis), a nulla rileva l'uso che viene fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento del conseguimento indebito dei finanziamenti.

7.2.5 Reati introdotti dal D. Lgs. n. 75/2020: peculato mediante profitto dell'errore altrui ed abuso d'ufficio

Art. 316 c.p. Peculato mediante profitto dell'errore altrui

"Il pubblico ufficiale o l'incaricato di un pubblico servizio, il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità, è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da sei mesi a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000"

Brevi cenni sulla fattispecie

Il presupposto è rappresentato dall'esistenza di un errore da parte del soggetto offerente. Significa che un rappresentante della Pubblica Amministrazione, ovvero un privato, deve erroneamente consegnare denaro a altra utilità ad un pubblico ufficiale o a un incaricato di pubblico servizio. La dazione deve essere spontanea, dunque causalmente ricollegabile – in via esclusiva – all'errore. Non deve quindi essere determinata da alcun comportamento fraudolento eventualmente serbato da parte del pubblico ufficiale o dell'incaricato di pubblico servizio che vadano poi a ricevere la *res*.

Art. 323 c.p. Abuso d'ufficio

"Salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto, è punito con la reclusione da uno a quattro anni. La pena è aumentata nei casi in cui il vantaggio o il danno hanno carattere di rilevante gravità."

Brevi cenni sulla fattispecie

L'elemento materiale che caratterizza l'abuso d'ufficio si risolve in una condotta di abuso che deve essere necessariamente realizzata nello svolgimento delle funzioni e del servizio (Cass. VI, n. 1269/2012) e che si concretizza:

a) attraverso la violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità ovvero, in alternativa,
b) mediante l'inosservanza di un obbligo di astensione.

La condotta abusiva deve essere diretta a procurare, intenzionalmente, a sé o ad altri un ingiusto vantaggio patrimoniale oppure a procurare ad altri un danno ingiusto.
La violazione di specifiche regole di condotta espressamente previste dalla legge o d atti aventi forza di legge e dalle quali non residuino margini di discrezionalità si ha quando il comportamento del soggetto attivo contrasta con norme di legge

che regolano l'esercizio del potere pubblico. In sostanza, l'abuso d'ufficio si configura soltanto in relazione all'attività dei pubblici agenti che, nel compiere l'atto, non usufruiscano di margini di discrezionalità, con la conseguenza che la condotta abusiva – connotata dall'insussistenza di tale ultimo elemento e commessa in violazione di specifiche regole di condotta che disciplinano la funzione o il servizio, si risolve nel realizzare esclusivamente un interesse antitetico con quello per il quale il potere è stato conferito (Cass. S.U., n. 155/2011).

7.2.6 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria

Art.377 – bis c.p.: "*Salvo che il fatto non costituisca più grave reato, chiunque, con violenza, minaccia o con offerta o promessa di denaro o altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere, è punito con la reclusione da due a sei anni*".

Brevi cenni sulla fattispecie

Come più sopra indicato si è ritenuto di trattare questo reato nella presente Parte Speciale, pur se prevista in un articolo del d.lgs. 231/01 diverso da quelli espressamente diretti a tutelare la Pubblica Amministrazione ed il suo patrimonio, per una affinità di bene protetto dalla fattispecie di cui all'art. 377 bis c.p.

Infatti, l'interesse tutelato dalla fattispecie è il corretto svolgimento dell'attività giudiziaria, attività che rientra tra i principali poteri attribuiti allo Stato dalla nostra Costituzione. Ma non solo. L'art. 377 bis si trova in una sorta di continuità logica con l'art. 319 ter c.p. "Corruzione in atti giudiziari".

La corruzione in atti giudiziari si concretizza sia quando la corruzione si realizza nei confronti di un magistrato, un cancelliere o un altro funzionario che svolge la sua attività per il sistema giudiziario sia quando la corruzione è rivolta al testimone. Infatti, al testimone è attribuita la qualifica di Pubblico Ufficiale al momento della sua deposizione (da ultimo C. Cass., S.U., 25 febbraio 2010, n. 15208). Inoltre, la testimonianza deve considerarsi "atto giudiziario", essendo è atto funzionale ad un procedimento giudiziario (C.Cass. S.U., cit).

Invece, il delitto di cui all'art. 377 bis c.p., prevede che il soggetto indotto a non rendere dichiarazioni o a renderle mendaci sia una persona che possa avvalersi della facoltà di non rispondere: tra questi rientrano imputati di reati connessi o collegati, ossia soggetti che sono indagati o imputati nello stesso procedimento penale in cui gli stessi rendono dichiarazioni, ovvero in procedimenti che abbiano rispetto a quest'ultimo un collegamento probatorio.

Per la sussistenza di entrambe le ipotesi è necessario che il corruttore prometta o offra denaro o altra utilità al soggetto che deve rendere dichiarazioni.

7.3 Destinatari ed obiettivi della presente parte speciale

La presente Parte Speciale disciplina i comportamenti posti in essere da amministratori e dipendenti di Digitronica.IT S.p.A. nell'ambito dei rapporti con la Pubblica Amministrazione.

Tutti i destinatari devono applicare ed osservare le regole di condotta prescritte dalla presente Parte Speciale, nonché adottare comportamenti idonei al fine di prevenire il verificarsi dei reati oggetto della stessa.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- fornire le «regole di comportamento» e le procedure che gli amministratori, i dirigenti ed i dipendenti, sono tenuti ad osservare ai fini della corretta applicazione del Modello;
- fornire ai responsabili delle funzioni aziendali ed all'Organismo di Vigilanza gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

7.4 I "processi sensibili" nei rapporti con la Pubblica Amministrazione con riferimento alle categorie di reati di cui agli artt. 24 e 25 D. Lgs. 231/2001

Con riferimento a tutti i reati sopra descritti, le attività che sono state ritenute esposte maggiormente a rischio, ovvero i «principali processi sensibili» che comportano rapporti diretti con la Pubblica Amministrazione, sono sostanzialmente riconducibili alle categorie sottoelencate.

Corruzione e concussione

Il delitto di corruzione è in astratto realizzabile tutte le volte in cui i soggetti che operano per Digitronica.IT S.p.A. si trovano in contatto diretto con la Pubblica Amministrazione.
Invece, il profilo di rischio relativo al delitto di concussione pare essere irrilevante posto che dovrebbe essere realizzato nell'interesse o a vantaggio della Società da un soggetto appartenente alla stessa. Ciò è incompatibile con la struttura del reato di concussione, che vede come unico soggetto attivo il Pubblico Ufficiale o l'Incaricato di Pubblico Servizio.

Discorso diverso deve essere fatto con riferimento al reato di cui all'art. 319 quater c.p. Infatti, se nella "costrizione", di cui al delitto di concussione, si ravvisa una violenza psichica che non rende punibile il cittadino che la subisce, analogo ragionamento non può essere fatto rispetto all'induzione, essendo questo un sopruso indiretto ed immediato cui il soggetto privato può non dar seguito e che, tuttavia, si attiva, comprendendo il messaggio e provvedendo a darvi corso.
Sulla base di queste osservazioni, con riferimento alle ipotesi corruttive, sono stati individuati i seguenti "processi sensibili":

- attività dirette all'ottenimento o al rinnovo di autorizzazioni, concessioni e licenze per l'esercizio delle attività aziendali;
- • rapporti ordinari con Enti pubblici nell'ambito dello svolgimento delle attività aziendali (ad es. rapporti con l'amministrazione finanziaria, con l'Ufficio della Dogane, INPS, INAIL, etc.);
- gestione delle verifiche e ispezioni da parte degli Enti Pubblici di controllo (amministrative, fiscali, previdenziali, relative all'igiene e sicurezza sul lavoro, alla materia ambientale, etc.).

Inoltre, sono state identificate le seguenti "attività strumentali" per una eventuale realizzazione dei reati in commento:

- gestione dei flussi finanziari e di tesoreria (ciclo attivo, ciclo passivo, flussi di cassa, contabilità)
- gestione del rapporto con il personale dipendente (assunzioni, rimborsi spese, etc);
- scelta e gestione dei fornitori;
- gestione delle risorse umane;
- gestione dei contratti di agenzia.

Truffa aggravata ai danni dello Stato

In relazione a tali reati, si ritiene che le eventuali "attività sensibili" siano configurabili quando la Società partecipa a procedure per l'ottenimento di erogazioni, contributi, finanziamenti o altre agevolazioni patrimoniali erogati da organismi pubblici italiani o comunitari.

Più precisamente, in tali contesti sono considerate "sensibili" le attività di preparazione della documentazione necessaria ad ottenere le suddette agevolazioni di natura patrimoniale.

Frode informatica

Il rischio rispetto a questo tipo di reato potrebbe - seppur molto astrattamente - sussistere, concretizzandosi in un'alterazione di *data base* della Pubblica Amministrazione, quali, ad esempio, quelli relativi ai dati fiscali o previdenziali dell'azienda, che sono accessibili direttamente dal contribuente.

Inoltre, esiste un minimo profilo di rischio quando la Società partecipa a procedure per l'ottenimento di agevolazioni di natura patrimoniale che la Pubblica Amministrazione indice on-line.

Si ritiene che tale area di rischio sia adeguatamente fronteggiata con l'organizzazione interna, le procedure previste dalla Società per la gestione dei sistemi informatici e tutta la documentazione richiamata alla successiva Parte dedicata ai reati informatici.

Ipotesi di malversazione o di indebita percezione di erogazioni pubbliche

Digitronica.IT S.p.A. partecipa a procedure per l'ottenimento di erogazioni, contributi/finanziamenti/mutui agevolati da parte di organismi pubblici italiani o comunitari ed ha individuato, in questo contesto, quale attività a rischio, la predisposizione della documentazione di rendicontazione al fine di dimostrare l'utilizzo dei fondi ricevuti.

Corruzione in atti giudiziari ed induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria

I rischi relativi a tali fattispecie paiono essere praticamente irrilevanti e potrebbero sussistere solo in presenza di un procedimento giudiziario. Si ritiene che la gestione delle attività sensibili strumentali alla commissione dei delitti contro la P.A. possa impedire, tramite la trasparenza della gestione finanziaria, eventuali attività dirette alla corruzione di soggetti che esercitino funzioni giudiziarie, come sopra richiamate, ovvero all'induzione a tacere o a dichiarare il falso nei confronti dei soggetti di cui all'art. 377 bis c.p.

In ogni caso, Digitronica.IT S.p.A. ritiene che il rispetto dei principi generali elencati nel MOG e nel codice etico possa arginare adeguatamente tale teorico rischio.

Gestioni diverse dello stesso, che magari impongano la comunicazione a determinati soggetti appartenenti alla Società dell'esistenza di un procedimento penale e del ruolo ricoperto da altri soggetti all'interno dello stesso, potrebbero alterare il clima di serenità necessario per affrontare adeguatamente tale circostanza e creare anche solo un mero condizionamento psicologico considerato del tutto inopportuno.

7.5 Principi generali e regole di comportamento

Al fine di garantire la massima trasparenza e correttezza nell'ambito dei rapporti che Digitronica.IT S.p.A. intrattiene, a qualsiasi titolo, con soggetti appartenenti a Pubbliche Amministrazioni, di matrice nazionale, comunitaria ed

internazionale, sono stati elaborati alcuni principi generali di comportamento cui i Destinatari del Modello devono rigorosamente attenersi nello svolgimento delle loro specifiche attività.

I seguenti divieti di carattere generale si applicano agli organi sociali, ai dirigenti e ai dipendenti della Società.

Conformemente a quanto previsto nel Codice Etico, nelle procedure, e nelle norme aziendali, al fine di instaurare e mantenere ogni rapporto con la P.A. sulla base di criteri di massima correttezza e trasparenza, ai suddetti soggetti è fatto divieto di:

- porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali che, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale;
- violare i principi e le procedure aziendali elaborate dalla Società per prevenire i reati nei rapporti con la P.A.

Più in particolare, nella gestione della normale attività aziendale è sempre vietato:

- distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore, anche nei contesti sociali in cui tali pratiche costituiscono una prassi. In ogni caso, tale prassi è sempre vietata quando possano influenzarne l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'Azienda;
- effettuare elargizioni in denaro;
- promettere o versare somme o beni in natura a qualsiasi soggetto (sia esso un dirigente, funzionario o dipendente della P.A.) per promuovere o favorire gli interessi della Società, anche a seguito di illecite pressioni;
- accordare vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della P.A. italiana o straniera che possano promuovere o favorire gli interessi della Società;
- effettuare prestazioni o riconoscere compensi in favore dei consulenti, dei collaboratori esterni, dei partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e nella prassi vigente in ambito locale;
- ricevere o sollecitare elargizioni in denaro, omaggi, regali, o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia;
- ricorrere a forme diverse di aiuti, contributi o atti di liberalità che, sottoveste di sponsorizzazioni, incarichi, consulenze o pubblicità abbiano invece le stesse finalità sopra vietate;
- creare fondi a fronte di beni/servizi contrattualizzati a prezzi superiori a quelli di mercato oppure di fatturazioni inesistenti in tutto o in parte;
- effettuare pagamenti in contante o in natura, ad eccezione delle operazioni di valore economico modesto stabilite dalla direzione aziendale;
- presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi, finanziamenti agevolati o aggiudicazioni illecite di procedure di gara indette da enti pubblici;
- destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;

- alterare la rendicontazione relativa alla gestione delle suddette somme;
- alterare e/o utilizzare abusivamente e in modo improprio i sistemi informatici aziendali. Più precisamente è fatto divieto di utilizzare tale patrimonio societario per fini personali, ovvero con lo scopo di alterare dati e comunicazioni inerenti sotto qualsiasi aspetto l'attività dell'Azienda.

Al fine di garantire il rispetto del Modello, con particolare riguardo a quanto previsto dalla presente Parte speciale, la Società non inizierà o proseguirà nessun rapporto con esponenti aziendali, collaboratori esterni, fornitori o partner che non intendano allinearsi al principio della stretta osservanza delle leggi e dei regolamenti in tutti i Paesi in cui la società opera.

7.6 Procedure specifiche di comportamento da applicare nelle "attività sensibili"

In seguito all'analisi dei rischi, Digitronica.IT S.p.A. ha ritenuto opportuno implementare il sistema di gestione delle attività aziendali e di controlli interni con l'elaborazione di alcuni protocolli finalizzati a ridurre il rischio di commissione dei reati relativi alla presente Parte Speciale.

Questi sono:

- gestione dei rapporti e degli adempimenti verso la Pubblica Amministrazione (quali, a titolo esemplificativo, la gestione degli adempimenti in materia tributaria, la gestione del contenzioso giudiziale o amministrativo, la gestione degli adempimenti di legge in materia di trattamenti previdenziali ed assistenziali del personale dipendente, la gestione degli adempimenti in materia di salute, sicurezza, igiene degli impianti e dei luoghi di lavoro, la gestione dei rapporti con i funzionari pubblici degli Enti competenti in materia fiscale, sanitaria, di sicurezza pubblica, la gestione dei rapporti con gli altri enti pubblici per l'ottenimento di autorizzazioni, licenze, provvedimenti amministrativi e permessi necessari per l'esercizio delle attività aziendali e la gestione delle ispezioni amministrative, fiscali, previdenziali, in materia antinfortunistica ecc.);
- l'approvvigionamento di beni, servizi e prestazioni;
- la gestione dei rapporti con agenti, intermediari, clienti e fornitori;
- la gestione di incassi e pagamenti e la gestione della contabilità;
- la gestione dei rimborsi spese a dipendenti e collaboratori;
- la richiesta e la gestione di finanziamenti;
- la gestione delle assunzioni del personale dipendente e parasubordinato;
- la gestione dell'erogazione di bonus, premi ed omaggi.

I Destinatari del Modello sono tenuti, unitamente al rispetto dei principi generali espressi ed a quelli sanciti nel Codice Etico, alla stretta osservanza delle procedure che costituiscono parte integrante del Modello di Digitronica.IT S.p.A.

7.7 I controlli dell'Organismo di Vigilanza

Il sistema di controllo predisposto da Digitronica.IT S.p.A. prevede la supervisione ad opera dell'Organismo di Vigilanza, soggetto istituzionalmente preposto alla verifica dell'idoneità ed efficacia del modello.

L'OdV, pertanto, effettua periodicamente specifici controlli sulle attività connesse ai "processi sensibili" al fine di verificare il rispetto dei Principi Generali di comportamento e delle procedure e delle istruzioni operative come sopra indicate.

Inoltre, è stata redatta specifica procedura che regolamenta i flussi informativi nei confronti dell'OdV, al fine di fornire allo stesso le informazioni necessarie per l'espletamento dell'attività di verifica e controllo, nel rispetto della normativa sul c.d. *whistleblowing*.

In ogni caso, all'OdV vengono garantiti autonomi poteri di iniziativa e controllo e potrà avere accesso in qualunque momento a tutta la documentazione aziendale ritenuta rilevante. Nell'ambito dei propri poteri potrà indire, a sua discrezione, riunioni specifiche con i soggetti deputati alla gestione dei "processi sensibili" e potrà attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato presente Modello.

Organizzazione

Digitronica.IT S.p.A.

Sede: Viale del Lavoro, 52 Verona
Phone: 045 50 19 01
Fax: 045 50 22 58
Email: info@digitronica.it
Pec: digitronica.it@pec.it

MOGC 231 – PARTE SPECIALE

ai sensi del D.Lgs.n.**231** del 8 Giugno 2001 e s.m.i.

Master	☐
Copia controllata	☐
Copia non controllata	☐
Numero della copia	☐

Emissione DG	Data		Firma	
Approvazione DG	Data		Firma	
Approvazione ODV	Data		Firma	

Stato delle revisioni

Versione	Data	Descrizione	Autore
00	*04/06/2019*	Prima emissione	Digitronica.IT Srl
01	*01/12/2020*	Aggiornamento	Digitronica.IT S.p.A.
02	*01/04/2022*	Aggiornamento	Digitronica.IT S.p.A.
03	*22/01/2024*	Aggiornamento OdV	Digitronica.IT SpA

Indice generale della sezione

Modello di Organizzazione, Gestione e Controllo – Parte speciale

8.1 Introduzione e funzione della parte speciale dei delitti in materia di strumenti di pagamento diversi dai contanti

Nella presente Parte Speciale vengono esaminati i profili di rischio relativi ai reati presupposto che rientrano nella categoria dei delitti in materia di strumenti di pagamento diversi dai contanti, ovvero tutti i reati elencati nell'art. 25 octies.1 del d.lgs. 231/2001.

8.2 Le fattispecie di reato richiamate dal D.Lgs.n.231/2001

La conoscenza della struttura e delle modalità realizzative delle fattispecie di reato, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D. Lgs. 231/2001 è collegato il regime di responsabilità a carico dell'Ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

Si riportano, pertanto, i riferimenti normativi e le descrizioni dei reati oggetto della presente Parte Speciale.

Art. 493 *ter* c.p. Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti

Tale disposizione punisce chi, al fine di trarne profitto per sé o per altri, utilizzi indebitamente, falsifichi o alteri carte di credito o di pagamento, documenti analoghi che abilitino al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero ogni altro strumento di pagamento diverso dai contanti. L'art. 493-ter c.p. punisce altresì chiunque *"possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi".*

Art. 493 *quater* c.p. Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti

Reato introdotto dal D. Lgs. 184/2021, che punisce chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produca, importi, esporti, venda, trasporti, distribuisca, metta a disposizione o in qualsiasi modo procuri a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

Art. 640 *ter* c.p. Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale

Tale delitto era già stato previsto nel D. Lgs. 231/2001 quale reato presupposto dell'illecito amministrativo di cui all'art. 24 (indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture), ma con una rilevanza per l'ente circoscritta alle sole ipotesi di frode informatica commessa in danno dello Stato o di altro ente pubblico, e non quando commesso in danno di soggetti privati.
Con il D. Lgs. 184/2021, invece, gli enti potranno essere ritenuti responsabili (questa volta ai sensi dell'art. 25-octies.1)

anche per la commissione di frodi informatiche commesse a danno di privati, ma a condizione che sia prospettabile l'aggravante di un fatto illecito che abbia prodotto un trasferimento di denaro, di valore monetario o di valuta virtuale.

Quanto alle sanzioni comminabili all'ente in caso di realizzazione di questi nuovi reati presupposto, l'art. 25-octies.1 prevede una sanzione pecuniaria da 300 a 800 quote per il delitto di cui all'art. 493-ter c.p. e fino a 500 quote per i delitti di cui agli artt. 493-quater e 640-ter, nella predetta ipotesi aggravata.
Al secondo comma, poi, l'art. 25-octies.1 stabilisce che, salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offenda il patrimonio previsto dal codice penale, avente ad oggetto strumenti di pagamento diversi dai contanti, all'ente si applicherà la sanzione pecuniaria:
• fino a 500 quote, se il delitto è punito con la pena della reclusione inferiore ai dieci anni;
• da 300 a 800 quote, se il delitto è punito con la pena non inferiore ai dieci anni di reclusione. In questo modo, pur adottando una tecnica legislativa che farà certamente discutere quanto al rispetto dei principi di legalità, tassatività e determinatezza, il legislatore apre le porte ad una serie potenzialmente molto ampia di reati relativi alla gestione di strumenti di pagamento diversi dai contanti.
Infine, in aggiunta alle sanzioni pecuniarie sopra citate, nelle ipotesi di condanna per tali reati si applicheranno all'ente anche le sanzioni interdittive previste dall'art. 9, comma 2, del D. Lgs. 231/2001 che, a seconda dei casi, andranno dal divieto di pubblicizzare beni o servizi all'interdizione dall'esercizio dell'attività.

8.3 Destinatari ed obiettivi della presente parte speciale

La presente Parte Speciale disciplina i comportamenti posti in essere da amministratori e dipendenti di Digitronica.IT S.p.A. che potrebbero comportare la commissione, a vantaggio della Società, dei reati sopra identificati.
Tutti i destinatari devono applicare ed osservare le regole di condotta prescritte dalla presente Parte Speciale, nonché adottare comportamenti idonei al fine di prevenire il verificarsi dei reati oggetto della stessa.
Nello specifico, la presente Parte Speciale ha lo scopo di:

- fornire le «regole di comportamento» e le procedure che gli amministratori, i dirigenti ed i dipendenti, sono tenuti ad osservare ai fini della corretta applicazione del Modello;
- fornire ai responsabili delle funzioni aziendali ed all'Organismo di Vigilanza gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

8.4 I "processi sensibili" in materia di pagamenti con strumenti diversi dai contanti con riferimento ai reati di cui all'art. 25octies.1 D. Lgs. 231/2001

Con riferimento ai delitti sopra elencati, sono stati individuati i seguenti "processi sensibili":

- gestione, diretta o indiretta, degli strumenti di pagamento e dei movimenti monetari tra i quali, ad esempio, la riscossione delle vendite mediante strumenti di pagamento diversi dai contanti, come le vendite online o quelle effettuate tramite i punti vendita che utilizzano dispositivi elettronici che consentono di effettuare pagamenti

mediante moneta elettronica, carte di credito, di debito o prepagate.

8.5 Principi generali e regole di comportamento

Al fine di garantire la massima trasparenza e correttezza nello svolgimento dell'attività di Digitronica.IT S.p.A., sono stati elaborati alcuni principi generali di comportamento cui i Destinatari del Modello devono rigorosamente attenersi nello svolgimento delle loro specifiche attività.

I seguenti divieti di carattere generale si applicano agli organi sociali, ai dirigenti e ai dipendenti della Società.
Conformemente a quanto previsto nel Codice Etico, nelle procedure e nelle norme aziendali, ai suddetti soggetti è fatto divieto di:

- porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali che, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale;
- violare i principi e le procedure aziendali elaborate dalla Società per prevenire i reati di cui sopra.

Più in particolare, nella gestione della normale attività aziendale dovranno essere rispettate le prescrizioni previste nei protocolli adottati con il presente Modello, nel rispetto delle deleghe interne conferite e custodite presso la Società stessa.

8.6 Procedure specifiche di comportamento da applicare nelle "attività sensibili"

In seguito all'analisi dei rischi, Digitronica.IT S.p.A. ha ritenuto opportuno implementare il sistema di gestione delle attività aziendali e di controlli interni con l'elaborazione di alcuni protocolli finalizzati a ridurre il rischio di commissione dei reati relativi alla presente Parte Speciale. Ciò, con particolare riferimento a tutti quei processi aziendali che riguardano la movimentazione dei flussi finanziari attivi e passivi della Società.

I Destinatari del Modello sono tenuti, unitamente al rispetto dei principi generali espressi ed a quelli sanciti nel Codice Etico, alla stretta osservanza delle procedure che costituiscono parte integrante del Modello di Digitronica.IT S.p.A.

8.7 I controlli dell'Organismo di Vigilanza

Il sistema di controllo predisposto da Digitronica.IT S.p.A. prevede la supervisione ad opera dell'Organismo di Vigilanza, soggetto istituzionalmente preposto alla verifica dell'idoneità ed efficacia del modello.

L'OdV, pertanto, effettua periodicamente specifici controlli sulle attività connesse ai "processi sensibili" al fine di verificare il rispetto dei Principi Generali di comportamento e delle procedure e delle istruzioni operative come sopra indicate.

Inoltre, è stata redatta specifica procedura che regolamenta i flussi informativi nei confronti dell'OdV, al fine di fornire allo stesso le informazioni necessarie per l'espletamento dell'attività di verifica e controllo, nel rispetto della normativa sul c.d. *whistleblowing*.

In ogni caso, all'OdV vengono garantiti autonomi poteri di iniziativa e controllo e potrà avere accesso in qualunque momento a tutta la documentazione aziendale ritenuta rilevante. Nell'ambito dei propri poteri potrà indire, a sua discrezione, riunioni specifiche con i soggetti deputati alla gestione dei "processi sensibili" e potrà attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato presente Modello.