MODELLO ORGANIZZATIVO, DI GESTIONE E CONTROLLO

ai sensi del Decreto Legislativo 8 giugno 2001 n. 231

PARTE SPECIALE

Approvazione	Delibera del Consiglio di Amministrazione del 29.03.2023

SardegnaIT S.r.l. c.s.u.
Sede legale e operativa
Via dei Giornalisti 6, 09122 Cagliari
C.F., P.IVA e iscr. CCIAA Cagliari 03074520929

tel: +39 070 606 9015 - fax: +39 070 606 9016
mail: info@sardegnait.it
pec: segreteria@pec.sardegnait.it
web: www.sardegnait.it

Sommario

PARTE SPECIALE - PREMESSA

Destinatari della Parte Speciale

La Parte Speciale stabilisce quali comportamenti debbano tenere i Destinatari coinvolti nelle Aree Sensibili e nei Processi Sensibili. Obiettivo della regolamentazione è che tutti i soggetti interessati tengano comportamenti conformi a quanto prescritto, al fine di prevenire la commissione dei Reati Presupposto ritenuti a rischio di accadimento rilevante.

I Destinatari, oltre che alle prescrizioni della Parte Speciale, dovranno ovviamente attenersi anche ai Principi Generali e alle regole contenuti nella Parte Generale del Modello, nel Codice Etico, nei protocolli e/o procedure, allegati al modello e nelle specifiche procedure interne della società, denominate ILA e PRO.

Sistema di organizzazione

I componenti degli organi sociali e i dipendenti muniti di poteri verso l'esterno devono agire nei limiti dei poteri ad essi conferiti. I dipendenti privi di poteri verso l'esterno devono richiedere l'intervento dei soggetti muniti di idonei poteri.

In linea generale, il sistema di organizzazione della società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, di segregazione delle funzioni e dei ruoli in modo che nessun soggetto possa gestire da solo un intero processo (anche per quanto attiene la possibilità di maneggio di risorse finanziarie), in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

Le linee di comportamento si applicano sia ai dipendenti e ai componenti degli organi sociali di Sardegna IT S.r.l. c.s.u., in via diretta, sia alle società di servizi, ai consulenti, ai fornitori e ai partner a vario titolo, in forza di apposite clausole contrattuali.

Suddivisione della Parte Speciale

La Parte speciale è suddivisa in Sezioni, dedicate alle Aree Sensibili in relazione alle diverse tipologie di Reati Presupposto ritenuti a rischio rilevante di commissione.

Allegati

Sono allegati alla Parte speciale del modello i seguenti documenti:

1) "SCHEDA DI MODALITÀ DI COMMISSIONE DEL REATO";

2) "*protocolli* e procedure"

- **2a)** protocollo contabilità e bilancio;
- **2b)** protocollo ispezioni e verifiche.

PARTE SPECIALE – SEZIONE PRIMA

Aree Sensibili: mappatura e processi strumentali/funzionali

La matrice delle Aree Sensibili individuate

La mappatura realizzata da Sardegna IT S.r.l. c.s.u. è riportata nella "Mappatura dei reati e delle attività e modalità di commissione del reato" che è parte integrante e essenziale del presente modello.

In particolare i macro-processi primari dell'attività di Sardegna IT S.r.l. c.s.u. sono precisamente individuati nella su menzionata mappatura nella sezione denominata: "Attività a rischio reato", a cui si fa esplicito rinvio.

I Reati Presupposto potenzialmente configurabili nell'attività svolta da Sardegna IT S.r.l. c.s.u.

I Reati Presupposto a rischio di commissione rientrano nelle seguenti categorie:

1) Reati commessi nei rapporti con la Pubblica Amministrazione;

2) Delitti Informatici;

3) Delitti di criminalità organizzata;

4) Reati societari;

5) Reati di omicidio colposo e lesione colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;

6) Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;

7) Delitti in materia di violazione del diritto d'autore;

8) Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;

9) Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare;

10) Reati tributari.

Aree Sensibili in relazione agli altri Reati Presupposto.

Per quanto attiene gli altri Reati Presupposto la Società ha riscontrato che nello svolgimento dell'attività sociale non sono ravvisabili rischi rilevanti di commissione degli stessi.

La Società ritiene che per detti reati i principi del Codice Etico, i regolamenti, le disposizioni e le procedure interne siano sufficientemente idonei a prevenire o mitigare il rischio di commissione.

La Società svolgerà comunque un'attività di monitoraggio costante.

Regole di comportamento nell'ambito delle Aree Sensibili e dei Processi Sensibili

Per il dettaglio di dette regole si rinvia alle singole Sezioni di questa Parte Speciale.

Sardegna IT S.r.l. c.s.u. persegue il miglioramento delle proprie prestazioni, attraverso continuo monitoraggio e periodici audit interni e verifiche a campione volti a verificare l'applicazione del presente modello di gestione e controllo e la sua efficacia.

PARTE SPECIALE – SEZIONE SECONDA

Reati nei confronti della Pubblica Amministrazione

(art. 25 D.lgs. 231/2001)

Malversazione in danno dello stato o di altro ente pubblico; indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico

(art. 24 D.lgs. 231/2001)

Delitti di criminalità organizzata

(art. 24 ter D.lgs. 231/2001)

Le fattispecie di Reato Presupposto riconducibili alle tipologie dei reati (i) nei confronti della Pubblica Amministrazione (PA) e (ii) di malversazione e indebita percezione di erogazioni pubbliche, ritenute di rischio rilevante.

Si riporta qui di seguito una breve descrizione dei Reati Presupposto di cui trattasi.

(i) Reati Presupposto nei confronti della Pubblica Amministrazione

- **Peculato (art. 314 c.p.)**

  Il reato si configura nel caso in cui un pubblico ufficiale, o l'incaricato di un pubblico servizio[1], avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di danaro o di altra cosa mobile altrui, se ne appropria.

- **Peculato mediante profitto dell'errore altrui (art. 316 c.p.)**

  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.

- **Concussione (art. 317 c.p.)**

  Il reato si configura nel caso in cui un pubblico ufficiale, o l'incaricato di un pubblico servizio abusando dei suoi poteri o della sua qualità, costringe taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altre utilità. Per costrizione si intende qualunque violenza morale attuata con abuso di qualità e poteri che si risolva in una minaccia di un male ingiusto.

  Trattandosi di un reato proprio del pubblico ufficiale (o incaricato di pubblico servizio), nel quale il privato assume la figura di persona offesa/danneggiato da reato, l'eventualità che tale reato possa costituire un Reato Presupposto per la responsabilità diretta dell'ente appare residuale. Va soggiunto, che tali reati possono commettersi anche in concorso con un soggetto che non riveste la qualità di Pubblico ufficiale o di incaricato di Pubblico servizio.

  Pertanto, a titolo meramente esemplificativosi può ipotizzare il caso di un dipendente della Società concorra nel reato istigando un pubblico ufficiale a tenere un comportamento idoneo a configurare i reati sopra citati, sempre che sussista, naturalmente, il requisito dell'interesse o del vantaggio che la Società dovrebbe ritrarre da tale condotta.

---

[1] Si riporta la definizione di pubblico ufficiale e di incaricato di pubblico servizio fissata dal codice penale, utile anche ai fini dell'interpretazione degli altri articoli di legge appresso citati.

Art. 377 c.p. Nozione del pubblico ufficiale

«Agli effetti della legge penale, sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi».

Art. 358 Nozione della persona incaricata di un pubblico servizio:

«Agli effetti della legge penale, sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata, dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale.

- **Corruzione per l'esercizio della funzione o dei poteri (artt. 318 c.p.)**

  Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio riceva, per sé o per altri, denaro o altre utilità, ovvero ne accetta la promessa, per compiere atti nell'esercizio delle sue funzioni o dei suoi poteri. L'attività del pubblico ufficiale, in altre parole, si estrinseca in un atto conforme ai doveri d'ufficio (ad esempio: rilascio di un'autorizzazione dovuta).

  La pena si applica anche a chi dà o promette il denaro od altra utilità.

- **Corruzione per un atto contrario ai doveri d'ufficio (artt. 319 c.p.)**

  Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio riceva, per sé o per altri, denaro o altre utilità, ovvero ne accetti la promessa, per omettere o ritardare, o per aver omesso o ritardato, atti del suo ufficio (determinando un vantaggio per l'offerente). L'attività del pubblico ufficiale in altre parole si estrinseca nell'omissione di un atto d'ufficio ovvero in un atto contrario ai doveri d'ufficio (ad esempio: rilascio di un'autorizzazione in carenza di requisiti da parte del richiedente).

  La pena si applica anche a chi dà o promette il denaro od altra utilità.

  L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: accelerare i tempi per la conclusione di un iter autorizzativo di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: non irrogare una sanzione amministrativa a seguito dell'accertamento di una condotta illecita), sia in una condotta che, pur non concretizzandosi in uno specifico e predeterminato atto, rientri nell'esercizio delle funzioni del pubblico ufficiale (ad esempio: comunicare ad un Esponente Aziendale l'imminenza di una visita ispettiva in azienda).

  Tale ipotesi di reato si differenzia dalla concussione in quanto nella corruzione esiste tra corrotto e corruttore un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la costrizione del pubblico ufficiale.

- **Corruzione in atti giudiziari (art. 319-ter c.p.)**

  Il reato si configura quando i fatti di corruzione (v. artt. 318 e 319 c.p.) sono posti in essere per favorire o danneggiare una parte in processo civile, penale o amministrativo. Il fatto di reato è integrato anche nell'ipotesi che non via sia un ingiusto danno o un ingiusto vantaggio (l'ingiustizia della condanna dà luogo ad una circostanza aggravante). Nella nozione di pubblico ufficiale richiamata dalla norma vanno compresi oltre ai magistrati anche i loro collaboratori istituzionali (ad es. cancellieri).

- **Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)**

  Il reato si configura quando il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità. A differenza di quanto previsto per la concussione, il privato è punibile.

  Secondo la giurisprudenza, l'induzione indebita può consistere in un'attività di suggestione, persuasione o pressione morale posta in essere da un pubblico ufficiale o un incaricato di pubblico servizio nei confronti di un privato che, avvertibile come illecita da quest'ultimo, non ne annienta la libertà di determinazione, rendendo a lui possibile di non accedere alla pretesa del soggetto pubblico.

  La punibilità, oltre che per il pubblico ufficiale e l'incaricato di pubblico servizio, è prevista anche per il privato che, a differenza dell'ipotesi di concussione, non essendo obbligato ma solamente indotto alla promessa o dazione, conserva una possibilità di scelta criminale che giustifica l'applicazione di una pena.

- **Corruzione di persona incaricata di un pubblico servizio (art. 320 c. p.)**

  Tale ipotesi di reato si configura nel caso in cui un incaricato di pubblico servizio riceva o ne accetti la promessa, per sé o per un terzo, denaro o altra utilità per l'esercizio delle sue funzioni, per omettere o ritardare o avere omesso o ritardato un atto del suo ufficio ovvero per compiere o aver compiuto un atto contrario al suo dovere d'ufficio.

- **Pene per il corruttore (art. 321 c. p.)**

  La disposizione prevede che le pene stabilite nel primo comma dell'art. 318 c.p., nell'art. 319, nell'art. 319-bis, nell'art. 319 ter, e nell'art. 320 in relazione alle ipotesi di cui agli artt. 318 e 319 c.p. si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il danaro o altra pubblica utilità.

- **Abuso d'ufficio (art. 323 c.p.)**

  La condotta sanzionata è quella posta in essere dal pubblico ufficiale o dall'incaricato di pubblico sevizio (o, **se non riveste tale qualità**, **anche il concorrente nel reato**), nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste: **1)** dalla legge o **2)** da atti aventi forza di legge ,ed a condizione che da tali disposizioni non residuino margini di discrezionalità, ovvero, da colui che 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.

- **Istigazione alla corruzione (art. 322 c.p.)**

  Il reato si configura nel caso del privato che offre o promette denaro o altra utilità al pubblico ufficiale o all'incaricato di pubblico servizio, se l'offerta o la promessa non vengono accolte.

  L'istigazione è configurabile con riferimento sia alla corruzione per l'esercizio delle funzioni o dei poteri (art. 318 c.p.), sia alla corruzione per omettere o ritardare un atto di ufficio (art. 319 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 (art. 322-bis cod. pen.)**

  Sulla base del richiamo all'art. 322-bis operato dall'art. 25 del Decreto, le ipotesi di reato di corruzione e concussione summenzionate si configurano anche nel caso in cui il denaro o altra utilità è dato, offerto o promesso, anche a seguito di induzione a farlo:

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

  b) 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;

  c) 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;

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

  e) 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;

  f) alle 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.

- **Aumenti di pena**

  La legge 27 maggio 2015 n. 69 ha aumentato le pene per i reati di cui agli articoli 318 (corruzione per un atto d'ufficio), 319 (corruzione per omettere o ritardare un atto d'ufficio o commettere un atto contrario ai doveri d'ufficio), 319-ter (corruzione in atti giudiziari) e 319-quater (induzione indebita) codice penale, sopra menzionati.

- **Sanzioni interdittive per i reati di corruzione**

  La legge 19 gennaio 2019 n. 3 (modificando l'art. 25 del Decreto) ha inasprito le sanzioni interdittive per i reati di corruzione, differenziando il quantum sulla base del ruolo ricoperto all'interno dell'ente dal soggetto che ha commesso il delitto: per gli illeciti commessi dagli amministratori l'applicazione delle sanzioni interdittive è prevista da quattro a sette anni, mentre per gli illeciti commessi da persone sotto la vigilanza o il controllo di questi ultimi la sanzione è prevista da due a quattro anni.

- **Ravvedimento operoso per i reati di corruzione**

  La legge 19 gennaio 2019 n. 3 (inserendo nell'art. 25 del Decreto un nuovo comma 5-bis) ha introdotto uno sconto di pena per gli enti che, prima della sentenza di primo grado, si adoperino per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità trasferite e abbiano eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi.

- **Traffico di influenze illecite (art. 346-bis c.p.)**

  Il reato si configura allorché "chiunque, fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319-ter e nei reati di corruzione di cui all'articolo 322-bis, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322- bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri". Il reato è punito con la pena della reclusione da un anno a quattro anni e sei mesi.

  La stessa pena si applica a chi indebitamente dà o promette denaro o altra utilità.

  Sono previsti aumenti di pena nel caso di coinvolgimento di pubblici ufficiali o incaricati di pubblico servizio; la pena è invece diminuita se i fatti sono di particolare tenuità.

(ii) Reati Presupposto di malversazione e indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello stato o di un ente pubblico

- **Indebita percezione di erogazioni a danno dello Stato o di altro ente pubblico (art. 316-ter c.p.)**

  Il reato si configura a carico di 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, consegua 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.

  In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

  Il reato si consuma nel momento dell'ottenimento dei finanziamenti e si configura, con carattere residuale, solo nei casi in cui la condotta non integri gli estremi del reato di cui all'art. 640-bis c.p. (truffa aggravata per il conseguimento di erogazioni pubbliche) di cui appresso.

- **Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640 comma 2 n. 1, cod. pen.)**

  Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro ente pubblico o all'Unione Europea).

  Tale reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla P.A. informazioni non veritiere (es. documentazione artefatta), al fine di ottenere l'aggiudicazione della gara stessa.

- **Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)**

  Il reato si configura nel caso in cui la truffa (condotta di chi con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno: art. 640 c.p.) sia posta in essere per conseguire indebitamente 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. Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

- **Frode informatica (art. 640-ter c.p.)**

  Il reato si configura nel caso in cui un soggetto, 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. Di fatto, a titolo esemplificativo, il reato in esame può integrarsi qualora, una volta ottenuto un finanziamento, venga violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

- **Associazione per delinquere (art. 416 cod. pen.)**

  La condotta sanzionata dall'art. 416 cod. pen. è costituita dalla formazione e dalla permanenza di un vincolo associativo continuativo con fine criminoso tra tre o più persone, allo scopo di commettere una serie indeterminata di delitti, con la predisposizione di mezzi necessari per la realizzazione del programma criminoso e con la permanente consapevolezza di ciascun associato di far parte di un sodalizio e di essere disponibile ad operare per l'attuazione del programma delinquenziale.

  In sintesi, dunque, il reato associativo si caratterizza per tre elementi fondamentali, costituiti da:

  1) un vincolo associativo tendenzialmente permanente, o comunque stabile, destinato a durare anche oltre la realizzazione dei delitti concretamente programmati;

  2) l'indeterminatezza del programma criminoso;

  3) l'esistenza di una struttura organizzativa, sia pur minima, ma adeguata a realizzare gli obiettivi criminosi presi di mira.

  In particolare, sono puniti coloro che promuovono, costituiscono od organizzano l'associazione, per ciò solo, oltre a coloro che regolano l'attività collettiva da una posizione di superiorità o supremazia gerarchica, definiti dal testo legislativo come "capi".

  Sono puniti altresì con una pena inferiore tutti coloro che partecipano all'associazione.

- **Associazioni di tipo mafioso anche straniere (art. 416-bis cod. pen.)**

  Tale articolo punisce chiunque faccia parte di un'associazione di tipo mafioso formata da tre o più persone.

  L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne derivi per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

  Le pene sono aumentate:

  - per coloro che promuovono, dirigono, organizzano l'associazione;
  - nel caso in cui l'associazione è armata. L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito;
  - allorché le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti.

Le disposizioni del suddetto articolo si applicano anche alla camorra ed alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

- **Comportamenti da tenere nei rapporti con la Pubblica Amministrazione e con le Autorità Amministrative Indipendenti**

Interlocutori rientranti nella Pubblica Amministrazione

Le regole appresso descritte si applicano ai Destinatari che, a qualunque titolo,

e per conto o nell'interesse della Società, intrattengano rapporti con pubblici ufficiali, incaricati di pubblico servizio o, più in generale, con rappresentanti della Pubblica Amministrazione, con le Autorità di Vigilanza, con l'Autorità Giudiziaria, con Autorità Amministrative Indipendenti, italiane o estere, con le Forze dell'Ordine (di seguito "Rappresentanti della Pubblica Amministrazione").

È opportuno precisare che le regole di comportamento a cui debbono attenersi i Destinatari, si ispirano ad alcuni standard di controllo specifici, di riferimento, che qui di seguito vengono elencati:

1) Sistema di procedure di evidenza pubblica ex l. reg. 15 del 2008 per l'assunzione di personale e ove ritenuto necessario, nomina commissioni con almeno un componente esterno. Predisposizione di specifica procedura organizzativa per la gestione e formazione del personale.
2) Predisposizione di procedura per conferimenti di incarichi di consulenza ai sensi dell'atto di indirizzo per la gestione della Società. Nomina commissioni di valutazione anche con componenti esterni.
3) Istituzione dell'Albo fornitori qualificati e predisposizione di apposita procedura acquisti, secondo il Codice Appalti.
4) Predisposizione di specifiche procedure organizzative relative alla gestione missioni, gestione crediti e relativi contenziosi.
5) Osservanza delle prescrizioni di legge in tema di contratti pubblici. Individuazione del responsabile del procedimento per ciascuna gara. Composizione commissioni e tracciatura dei criteri.
6) Regolamentare l'accesso ai Sistemi Informativi della Pubblica Amministrazione attraverso un adeguato riscontro delle password di abilitazione e il rispetto della normativa sulla privacy.
7) Procedure di tracciabilità dei flussi finanziari aziendali con l'individuazione dei soggetti autorizzati all'accesso alle risorse.
8) Nella gestione dei rapporti con i soggetti richiedenti i contributi, adottare le procedure ai sensi delle leggi e dei regolamenti della Regione Sardegna.
9) Redigere apposita procedura per la gestione degli incubatori.
10) Controlli di completezza e correttezza della documentazione da presentare per la richiesta di finanziamenti/contributi (relativamente sia alla documentazione di progetto che alla documentazione attestante i requisiti tecnici, economici e professionali dell'azienda che presenta il progetto).
11) Nei rapporti con il socio unico (Regione Sardegna) gestire in maniera chiara e trasparente la tracciabilità degli incontri (relazioni, verbali, ecc.).
12) Nel processo di alienazione degli immobili devono essere rispettate le prescrizioni della proceduta di evidenza pubblica.

Processi sensibili

Si richiama quanto indicato nella Matrice dei Rischi allegata al presente Modello.

Poteri

Ai dipendenti ed ai componenti degli organi sociali che assumono obbligazioni attive e passive nei confronti della Pubblica Amministrazione, o che facciano richiesta di erogazioni pubbliche per conto di Sardegna IT S.r.l. c.s.u., deve essere attribuito formale potere in tal senso. I soggetti muniti di

poteri verso l'esterno devono agire nei limiti dei poteri ad essi conferiti. I soggetti privi di poteri verso l'esterno sono coordinati da persone munite di idonei poteri e, ove necessario, devono richiedere l'intervento dei soggetti muniti di idonei poteri.

Devono in ogni caso essere rispettate le procedure interne.

Comportamenti vietati

In linea generale, è fatto divieto ai Destinatari: *(i)* di 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; *(ii)* di porre in essere comportamenti in violazione dei principi e delle procedure e dei protocolli aziendali; *(iii)* di tenere comportamenti tali da influenzare in maniera impropria e/o illecita, in qualsiasi forma, le decisioni dei Rappresentanti della Pubblica Amministrazione e, in generale, dei terzi in relazione all'attività della Società.

In particolare, è fatto divieto ai Destinatari di:

- aderire a richieste o sollecitazioni indebite di denaro o di altre utilità che provengano, in forma diretta o indiretta, da Rappresentanti della Pubblica Amministrazione in cambio di prestazioni afferenti alle loro funzioni o qualifiche;
- promettere, offrire, effettuare ai Rappresentanti della Pubblica Amministrazione, direttamente o tramite terzi, elargizioni in denaro o altre utilità in cambio di favori, compensi o altri vantaggi per sé e/o per la Società;
- promettere, offrire, corrispondere a Rappresentanti della Pubblica Amministrazione o a loro familiari (anche in quei Paesi dove l'elargizione di doni rappresenta una prassi diffusa) omaggi e regali in qualsiasi forma (e pertanto anche in forma di ospitalità) al di fuori di quanto previsto dalla prassi aziendale e dal Codice Etico (vale a dire ogni forma di regalo non di modico valore, o eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). Gli omaggi consentiti debbono, in qualsiasi circostanza: *(i)* essere effettuati in relazione ad effettive finalità di business, *(ii)* risultare ragionevoli e in buona fede, *(iii)* essere registrati in apposita documentazione onde consentire le verifiche da parte dell'ODV; in nessun caso possono consistere in un somme di denaro.

La medesima disciplina si applica alle spese di rappresentanza. Pertanto, ai Destinatari è fatto divieto di:

- favorire, nei processi di acquisto, fornitori, consulenti o altri soggetti segnalati da Rappresentanti della Pubblica Amministrazione, in cambio di utilità per sé e/o per la Società, nonché procurare indebitamente, a sé, alla Società o a terzi, vantaggi di qualsivoglia natura a danno della Pubblica Amministrazione;
- accettare o ricevere omaggi o altri vantaggi, anche in denaro, volti a influenzare l'imparzialità e indipendenza del proprio giudizio;
- danneggiare fornitori in possesso dei requisiti richiesti nella selezione dell'appalto, (i) ricorrendo a criteri parziali, non oggettivi e pretestuosi, o(ii) disapplicando le disposizioni contrattuali, o (iii) accettando documentazione falsa o erronea, o (iv) scambiando informazioni sulle offerte degli altri fornitori, o (v) approvando requisiti inesistenti, o (vi) ricevendo servizi e forniture diverse da quelle contrattualmente previste;
- favorire, nei processi di assunzione e di selezione, dipendenti, collaboratori e consulenti, dietro specifica segnalazione dei Rappresentanti della Pubblica Amministrazione, in cambio di favori, compensi e/o altri vantaggi per sé e/o per la Società;
- effettuare/ricevere pagamenti e prestazioni in genere nei rapporti con collaboratori, clienti, fornitori, consulenti o altri soggetti terzi, che non trovino adeguata giustificazione nel rapporto contrattuale in essere ovvero in relazione al tipo di incarico da svolgere;
- ottenere incarichi, promettendo e/o elargendo utilità o vantaggio a favore di un Rappresentante della Pubblica Amministrazione;
- tenere una condotta ingannevole nei confronti della Pubblica Amministrazione, inviando documenti falsi, attestando requisiti inesistenti o fornendo garanzie non rispondenti al vero;
- presentare dichiarazioni non veritiere a Pubbliche Amministrazioni, nazionali e/o comunitarie, al fine di conseguire erogazioni pubbliche, quali ad esempio contributi, finanziamenti o altre agevolazioni;

- destinare finanziamenti pubblici a scopi diversi da quelli per cui sono stati concessi o redigere false rendicontazioni sul relativo utilizzo.

Obblighi dei Destinatari

È fatto obbligo ai Destinatari di attenersi alle seguenti prescrizioni:

- in caso di richieste di utilità da parte di un pubblico funzionario, il soggetto interessato ha l'obbligo di: (i) rifiutare ogni corresponsione, anche se sottoposto a pressioni; (ii) segnalare immediatamente l'accaduto al proprio responsabile o referente interno e all'Organismo di Vigilanza;
- in caso di conflitti di interesse che sorgano nell'ambito dei rapporti con la Pubblica Amministrazione, il soggetto interessato deve segnalare immediatamente l'accaduto al proprio responsabile o referente interno e all'Organismo di Vigilanza;
- in caso di dubbi circa la corretta attuazione delle regole comportamentali di cui sopra nel corso dello svolgimento delle attività operative, il soggetto interessato deve interpellare senza ritardo il proprio responsabile o il referente interno e, in assenza di risposta o qualora questa non sia risolutiva, inoltrare formale richiesta di parere all'Organismo di Vigilanza.

Ispezioni della Pubblica Amministrazione

Alle ispezioni da parte della Pubblica Amministrazione devono partecipare per la Società soggetti a ciò espressamente delegati. La Società è tenuta, nel corso di eventuali attività ispettive, a fornire la massima collaborazione all'espletamento degli accertamenti. In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati dell'ispezione ritengano necessario acquisire, previo consenso del responsabile aziendale responsabile dell'assistenza all'ispezione e delegato ad interloquire con l'autorità procedente. I verbali redatti dalle pubbliche autorità dovranno essere diligentemente conservati a cura della funzione aziendale che ha la responsabilità di seguire l'ispezione/verifica Ove opportuno, ai verbali delle autorità procedenti la funzione interessata potrà aggiungere verbali o rapporti ad uso aziendale interno. L'ODV deve essere informato dell'ispezione e, nel caso che il verbale conclusivo evidenziasse criticità, ne deve essere tempestivamente informato con nota scritta da parte del responsabile della funzione coinvolta.

Gare

Le disposizioni che seguono si applicano sia alla partecipazione a gare della Società sia, alle gare indette dalla Società, fermo in ogni caso il rispetto della normativa in vigore ancorché non richiamata.

La domanda deve contenere affermazioni rispondenti alla realtà, non deve omettere indicazioni dovute, non deve contenere informazioni fuorvianti o false.

La funzione preposta deve verificare che non sussistano in capo alla Società cause di esclusione dalla partecipazione alla gara previste dalle vigenti leggi[2].

È fatto divieto, in epoca anteriore alla gara e fino a che la stazione appaltante non abbia proceduto all'aggiudicazione della medesima, di intrattenere contatti:

Sono di norma vietate operazioni di pagamento in contanti, salvo casi esaurientemente documentati e per importi non superiori a 500,00 (cinquecento/00) euro e comunque non verso esponenti della Pubblica Amministrazione.

[2] Possono essere cause di esclusione dalla gara, a titolo esemplificativo: l'aver commesso gravi infrazioni debitamente accertate alle norme in materia di salute e sicurezza sul lavoro o in materia ambientale; la sussistenza di una situazione di conflitto di interesse; l'esistenza di situazioni distorsive della concorrenza; l'aver subito sanzioni interdittive ex D.lgs. 231/2001; il mancato rispetto delle norme sull'assunzione dei disabili; la sussistenza di una situazione di controllo rispetto ad altri partecipanti; la sussistenza di gravi illeciti professionale di cui all'art. 80, comma.5, lett. c) del codice dei contratti pubblici.

Sponsorizzazioni a favore della PA

Eventuali sponsorizzazioni attive o passive possono essere concesse soltanto in assenza di conflitto di interessi e previa autorizzazione dell'Amministratore delegato.

Conflitti di interesse

Qualunque criticità o conflitto di interesse che dovessero sorgere nell'ambito del rapporto con la Pubblica Amministrazione devono essere comunicati, per iscritto, anche all'ODV.

La Società provvede a raccogliere dai Destinatari che abbiano rapporti con la PA apposite dichiarazioni di assenza di conflitti di interesse.

Controlli

Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi ai Processi Sensibili di cui trattasi devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente eventuali situazioni di irregolarità o anomalie.

Codice Etico

Devono essere in generale osservate le disposizioni del Codice Etico e le indicazioni per le segnalazioni all'Organismo di Vigilanza.

Tracciabilità e trasparenza

La Società deve seguire, attribuendo opportuna evidenza, procedure che garantiscano tracciabilità e trasparenza delle scelte operate, mantenendo a disposizione dell'ODV tutta la documentazione di supporto.

Procedure

Devono essere osservati, e si richiamano, i protocolli e le Procedura allegati al presente Modello nonché le altre procedure interne della società.

I controlli dell'Organismo di Vigilanza

Devono essere osservati, e si richiamano, i protocolli e la Procedura allegati al presente Modello nonché le altre procedure interne della società.

PARTE SPECIALE - SEZIONE TERZA

Reati Societari

(Art. 25-ter D.lgs. n. 231/2001)

Le fattispecie di Reati Presupposto riconducibili alla tipologia dei reati societari, ritenute di rischio rilevante

Si riporta qui di seguito una breve descrizione dei Reati Presupposto societari ritenuti di rischio rilevante.

- **False comunicazioni sociali (art. 2621 c.c.)**

L'ipotesi di reato di cui all'art. 2621 c.c. si configura qualora «*Fuori dai casi previsti dall'art. 2622 (n.d.r.: concernente le società quotate), gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, …, 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, previste dalla legge, consapevolmente espongono fatti materiali rilevanti 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*».

È prevista la pena della reclusione da uno a cinque anni. La stessa pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

La norma è stata così modificata dalla legge 27 maggio 2015 n. 69 recante "*Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio*"[3].

- **Impedito controllo (art. 2625 c.c.)**

Il reato punisce gli amministratori che impediscono od ostacolano, mediante occultamento di documenti o con altri idonei artifici, lo svolgimento delle attività di controllo o di revisione attribuite ai soci, ad altri organi sociali, ovvero alle società di revisione, sempre che il fatto abbia cagionato un danno ai soci. In assenza di danno, il fatto costituisce illecito amministrativo e non genera responsabilità diretta dell'ente.

Si tratta di reato proprio degli amministratori.

- **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 di fusioni con altra società o di scissioni, che cagionino danno ai creditori.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato. Il reato è perseguibile a querela della persona offesa, che deve essere individuata in uno dei creditori danneggiati.

Si tratta di reato proprio degli amministratori.

---

[3] La citata legge n.69/2015 ha anche introdotto nel codice civile gli articoli 2621-bis e 2621-ter, che recitano rispettivamente

«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.

Salvo che costituiscano più grave reato, si applica la stessa pena di cui al comma precedente quando i fatti di cui all'articolo 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'articolo 1 del regio decreto 16 marzo 1942, 267 (n.d.r. si tratta dei piccoli imprenditori). In tale caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale».

«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 articoli 2621 e 2621-bis».

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

Il reato si configura quando viene formato o aumentato fittiziamente il capitale della società mediante *(i)* attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; *(ii)* sottoscrizione reciproca di azioni o quote; *(iii)* sopravvalutazione rilevante dei conferimenti dei beni in natura, dei crediti ovvero del patrimonio della società, nel caso di trasformazione.

Si tratta di reato proprio degli amministratori e dei soci conferenti.

- **Corruzione tra privati (art. 2635, comma 3, c.c.)**

La condotta criminosa prevista dall'art. 2635, 3° comma, c.c. consiste, salvo che il fatto costituisca più grave reato, nell'offrire, promettere o dare denaro o altra utilità non dovuti

  - ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori, di società o enti privati,
  - a coloro che nell'ambito organizzativo della società o dell'ente privato esercitano funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo,
  - a coloro che sono sottoposti alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma,

per far compiere o per far omettere un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà.

Si tratta di "corruzione attiva".

La corruzione è punita anche se perpetrata per interposta persona.

Il reato si applica anche a coloro che svolgessero le funzioni in via di fatto. Il reato è procedibile d'ufficio (art. 1, comma 5, Legge 9 gennaio 2019 n. 3).

La violazione degli obblighi inerenti all'ufficio si sostanzia nella violazione di obblighi istituzionali imposti dalla legge (es. obblighi la cui violazione integra i reati societari) o nella violazione di disposizioni regolamentari (es. statuti, deliberazioni assembleari, obblighi formali correlati a compiti funzionali). La violazione degli obblighi di fedeltà a sua volta è riferita a doveri contenuti in norme di legge, regolamentari o convenzionali, quali norme civilistiche (es. art. 2105, art. 1175, art. 1375 c.c.) ivi incluso l'astenersi dall'agire in conflitto di interessi.

La dazione o la promessa di denaro o altra utilità deve essere volta al compimento o all'omissione da parte del soggetto corrotto di un atto in violazione degli obblighi inerenti al suo ufficio o degli obblighi di fedeltà nei confronti della società di appartenenza.

Affinché si integri il reato di corruzione tra privati, è necessario che derivi un nocumento (per opinione della dottrina dominante anche di natura non patrimoniale) dal compimento o dall' omissione dell'atto nei confronti della società di appartenenza del corrotto.

- **Istigazione alla corruzione tra privati (art. 2635-bis c.c.)**

Il reato si configura quando l'offerta o la promessa corruttiva di cui sopra non siano accettate.

L'art. 2635 bis c.c., e introduce un'ipotesi speciale di tentata corruzione tra privati.

Per la configurazione del reato di corruzione tra privati (2635 c.c.) è necessario, l'accoglimento dell'offerta o della sollecitazione.

L'istigazione alla corruzione (art. 2635 bis c.c.) si perfeziona a seguito della mancata accettazione della sollecitazione o dell'offerta.

Il reato è procedibile d'ufficio (art. 1, comma 5, Legge 9 gennaio 2019 n. 3).

- **Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza (art. 2638 c.c.)**

Si tratta di un'ipotesi di reato che può essere realizzato con due condotte distinte:

1) la prima si realizza *(i)* attraverso l'esposizione nelle comunicazioni previste dalla legge alle Autorità Pubbliche di Vigilanza (al fine di ostacolare l'esercizio delle funzioni di queste ultime) di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero *(ii)* mediante l'occultamento,

con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati e concernenti la medesima situazione economica, patrimoniale o finanziaria. La responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;

2) la seconda si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza svolte da parte di pubbliche Autorità, attuato consapevolmente ed in qualsiasi forma, anche omettendo le comunicazioni dovute alle Autorità medesime.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori.

- **False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 Dlgs n. 19/2023)**

Chiunque, al fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all'articolo 29, forma documenti in tutto o in parte falsi, altera documenti veri, rende dichiarazioni false oppure omette informazioni rilevanti, è punito con la reclusione da sei mesi a tre anni. 2. In caso di condanna ad una pena non inferiore a mesi otto di reclusione segue l'applicazione della pena accessoria di cui all'articolo 32-bis del codice penale

La norma sanziona la condotta dei soggetti coinvolti nel processo di redazione dei documenti societari che, al fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all'articolo 29 d.lgs n.19/2023 (per operazioni societarie transfrontaliere di fusione, scissione e trasformazione) formano documenti in tutto o in parte falsi, alterano documenti veri, rendono dichiarazioni false oppure omettono informazioni rilevanti.

Norme relative a società quotate

Si ricorda per completezza che le seguenti norme riguardano soltanto le società quotate:

(i) art. 2622 c.c. (False comunicazioni sociali delle società quotate), nel nuovo testo come modificato dalla legge n. 69/2015 sopra menzionata, (ii) art. 173-bis del TUF (Falso in prospetto) e *(iii)* art. 2629-bis c.c. (Omessa comunicazione del conflitto di interesse).

Principi generali di comportamento

✓ **Destinatari**

Le disposizioni di questa Sezione si applicano ai Destinatari che, a qualunque titolo, siano coinvolti nelle Aree Sensibili rispetto ai reati societari sopra illustrati.

✓ **Gestione organi sociali e operazioni societarie**

Nello svolgimento delle operazioni attinenti alla gestione sociale, oltre alle regole di cui al Modello e, in particolare, a quelle indicate ai successivi paragrafi, i componenti degli organi sociali di Sardegna IT S.r.l. c.s.u. (e i dipendenti e consulenti nell'ambito delle attività da essi svolte) devono conoscere e rispettare:

- in generale, la normativa italiana e straniera applicabile;
- i principi contabili nazionali e internazionali;
- la struttura organizzativa aziendale e il sistema di controllo della gestione;
- le norme inerenti il sistema amministrativo, contabile, finanziario, di reporting della Società;
- il Codice Etico;
- le procedure/linee guida aziendali, la documentazione e le disposizioni inerenti;
- i regolamenti e i provvedimenti delle Autorità di controllo.

✓ **Obblighi e divieti dei soggetti coinvolti**

Obblighi per i Destinatari.

Le norme comportamemtali si ispirano ad alcuni standard di controllo specifici, di riferimento, che qui di seguito vengono elencati:

1.Prevedere uno o più incontri tra l'Organismo di Vigilanza e il Responsabile amministrativo, focalizzati sul bilancio, con eventuali approfondimenti ed analisi documentali di fattispecie di particolare rilievo e

complessità presenti nella bozza predisposta, curando la stesura del relativo verbale firmato da entrambi.

2.Prevedere almeno un incontro all'anno, in prossimità della riunione del Consiglio di Amministrazione, tra Organismo di Vigilanza e Collegio sindacale avente per oggetto il bilancio (con nota integrativa) con redazione di verbale.

3.Istituzione di riunioni periodiche tra Collegio Sindacale ed Organismo di Vigilanza per verificare l'osservanza della disciplina prevista in tema di normativa societaria.

4.Istituzione di una procedura chiara e con una specifica tempistica rivolta ai responsabili di funzione, con cui si stabilisca quali dati e notizie debbono essere forniti all'Amministrazione, nonché quali controlli devono essere svolti su elementi forniti dall'Amministrazione e da "validare".

5.Riporto periodico al Socio Unico sullo stato dei rapporti con il Collegio Sindacale e le altre Autorità abilitate ai controlli sulla Società.

6.Esistenza di un sistema definito di responsabilità aziendali e di deleghe coerenti.

7.Istituzione di una procedura volta a fornire ai soggetti aziendali alcune regole comportamentali da seguire nella gestione di rapporti con professionisti e soggetti appartenenti a società terze, che preveda regole predefinite per il conferimento di incarichi o consulenze a soggetti terzi, ispirandosi a criteri di legalità, trasparenza, condivisione funzionale, inerenza e giustificabilità.

8.Istituzione di una procedura per il controllo dei flussi finanziari e la tracciabilità dei pagamenti.

9.Adozione di uno o più strumenti normativi e/o organizzativi che nell'ambito della selezione, assunzione e gestione amministrativa del personale prevedano:

a. un processo di pianificazione delle risorse da assumere che tenga conto del fabbisogno;
b. l'individuazione dei requisiti minimi necessari (profilo) per ricoprire il ruolo e il relativo livello di retribuzione nel rispetto di quanto previsto dai Contratti Collettivi Nazionali del Lavoro (ove applicabili) ed in coerenza con le tabelle.

I Destinatari hanno l'obbligo di:

1. 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 ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
2. osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale e del patrimonio sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
3. assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale, nonché la libera e corretta formazione della volontà assembleare;
4. non porre in essere operazioni simulate o diffondere notizie false idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari;
5. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni che si rendessero necessarie nei confronti delle autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

Divieti per i Destinatari

È fatto divieto, in particolare, di:

• rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati sulla situazione economica, patrimoniale e finanziaria della Società non verificati con le strutture amministrative o lacunosi o comunque non rispondenti alla realtà;

• omettere o alterare dati ed informazioni imposti dalla legge in merito alla predisposizione dei bilanci di esercizio o comunque relativi alla situazione economica, patrimoniale e finanziaria della 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;

• 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 riserve legalmente non distribuibili;

• acquistare o sottoscrivere azioni della Società o di società controllate fuori dai casi previsti dalla legge, con lesione dell'integrità del capitale sociale;

• effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori;

• 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; è fatto altresì divieto di porre in essere comportamenti in violazione dei principi e delle procedure aziendali previste nella presente Sezione della Parte Speciale;

• porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino, lo svolgimento dell'attività di controllo e di revisione da parte del Collegio Sindacale o della società di revisione, o comunque di altri soggetti incaricati di controllo;

• 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;

• omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di Vigilanza, nonché omettere la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette Autorità;

• esporre nelle 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 delle autorità pubbliche di vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

Procedure

- **Tracciabilità delle scelte**

La Società deve seguire, attribuendo opportuna evidenza, procedure specifiche che garantiscano tracciabilità e trasparenza delle scelte operate, mantenendo a disposizione dell'ODV tutta la documentazione di supporto.

- **Procedure specifiche**

Devono essere osservati, e si richiamano, i protocolli e la Procedura allegati al presente Modello nonché le altre procedure interne della società.

- **Istigazione e Corruzione fra privati**

Con particolare riferimento al Reato Presupposto di corruzione fra privati, oltre ai protocolli ed alla procedura allegati al presente Modello e alle procedure interne, devono essere osservati anche i seguenti comportamenti:

è fatto divieto ai Destinatari di offrire, promettere o fare avere denaro o altre utilità a terzi per ottenere benefici in favore della Società. Allo stesso modo è fatto divieto di promettere, offrire, corrispondere a terzi o a loro familiari (anche in quei Paesi dove l'elargizione di doni rappresenta una prassi diffusa) omaggi e regali in qualsiasi forma (e pertanto anche in forma di ospitalità) al di fuori di quanto previsto dalla prassi aziendale e dal Codice Etico (vale a dire ogni forma di regalo non di modico valore, o eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). Gli omaggi consentiti debbono, in qualsiasi circostanza: (i) essere effettuati in relazione ad effettive finalità di business, (ii) risultare ragionevoli e in buona fede, (iii) essere registrati in apposita documentazione onde consentire le verifiche da parte dell'ODV; in nessun caso possono consistere in un somme di denaro. La medesima disciplina si

applica alle spese di rappresentanza.

La società provvede, inoltre, a raccogliere dai Destinatari apposite dichiarazioni di assenza di conflitti di interesse dei confronti dei contraenti. Qualunque criticità o conflitto di interesse che dovessero sorgere nell'ambito del rapporto con i contraenti devono essere comunicati, per iscritto, anche sall'ODV.

- **Comunicazioni ai soci o al pubblico**

Le comunicazioni al socio unico di dati relativi alla situazione economica, patrimoniale e finanziaria della Società (quali, a titolo esemplificativo, bilancio d'esercizio, relazioni trimestrali e semestrale, e simili) devono essere redatte secondo le specifiche procedure, prassi e logiche aziendali in essere, in modo da:

a) determinare con chiarezza e completezza i dati e le notizie che ogni funzione interessata deve fornire ed i criteri contabili per l'elaborazione dei dati;

b) individuare le suddette funzioni e gli argomenti oggetto di comunicazione e informativa, indicare idonee scadenze, prevedere l'organizzazione dei relativi flussi e l'eventuale rilascio di apposite certificazioni;

c) prevedere la trasmissione di dati ed informazioni alla funzione responsabile attraverso un sistema (anche informatico) che consente la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;

d) prevedere criteri e modalità per l'elaborazione dei dati del bilancio;

e) prevedere meccanismi condivisi nella formazione di dati statistici e stime.

- **Formazione**

In relazione alla predisposizione delle comunicazioni di cui alla presente Sezione è prevista la predisposizione di un programma di formazione di base, rivolto a tutti i responsabili delle funzioni coinvolte nella redazione del bilancio e degli altri documenti connessi, in merito alle principali nozioni e problematiche giuridiche (con particolare rilievo alle relative responsabilità penali) sul bilancio e sulle comunicazioni sociali di carattere economico patrimoniale e finanziario.

Rapporti con il Collegio Sindacale o con la società di revisione in ordine al controllo contabile e alla preparazione della situazione patrimoniale, economica e finanziaria di Sardegna IT S.r.l. c.s.u.

Nei rapporti tra Sardegna IT S.r.l. c.s.u. e il Collegio Sindacale o la società di revisione sono adottate le seguenti misure:

- rispetto delle procedure che regolamentano la fase di selezione delle proposte delle società di revisione contabile;
- salvo gli incarichi ed i compiti previsti per legge, alla società di revisione di Sardegna IT S.r.l. c.s.u. o ad altri soggetti ad essa collegati non possono essere attribuiti ulteriori diversi incarichi se non previa autorizzazione dell'Amministratore delegato.

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

Le attività della Società, ove soggette alla vigilanza di Pubbliche Autorità in base alle specifiche normative applicabili, devono essere svolte da funzioni all'uopo deputate ed individuate nelle disposizioni organizzative aziendali contenenti l'attribuzione di specifiche responsabilità con riferimento:

a) alle segnalazioni periodiche alle autorità previste da leggi e regolamenti;

b) alla trasmissione a queste ultime dei documenti previsti in leggi e regolamenti (ad es., bilanci e verbali delle riunioni degli organi sociali);

c) alla trasmissione di dati e documenti specificamente richiesti dalle autorità di vigilanza;

d) al comportamento da tenere nel corso degli accertamenti ispettivi. Tali procedure postulano le seguenti attività:

- 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;
- prestazione, nel corso dell'attività ispettiva, da parte delle funzioni e delle articolazioni organizzative ispezionate, della massima collaborazione all'espletamento degli accertamenti. In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati dell'ispezione ritengano necessario acquisire, previo consenso del responsabile aziendale responsabile dell'assistenza all'ispezione e delegato ad interloquire con l'autorità procedente;
- partecipazione alle ispezioni dei soggetti a ciò espressamente delegati. I verbali redatti dalle pubbliche autorità dovranno essere diligentemente conservati a cura della funzione aziendale che ha la responsabilità di seguire l'ispezione/verifica. Ove opportuno, ai verbali delle autorità procedenti la funzione interessata potrà aggiungere verbali o rapporti ad uso aziendale interno. Nel caso il verbale conclusivo evidenziasse criticità, anche l'ODV ne deve essere tempestivamente informato con nota scritta da parte del responsabile della funzione coinvolta.

Altre regole finalizzate alla prevenzione dei reati societari in genere.

Oltre a quanto sopra, dovranno essere previste riunioni periodiche dell'ODV con il Collegio Sindacale e l'organo preposto al controllo interno per verificare l'osservanza della disciplina in tema di normativa societaria.

I controlli dell'Organismo di Vigilanza

Si richiamano i contenuti *(i)* della Parte Generale relativi all'Organismo di Vigilanza e *(ii)* della Parte Speciale Sezione Undicesima.

PARTE SPECIALE – SEZIONE QUARTA

Delitti in materia di violazione del diritto d'autore e di pirateria informatica

(Art. 25-*novies* D.lgs. n. 231/2001)

Le fattispecie di Reati Presupposto riconducibili alla tipologia dei reati di violazione del diritto d'autore, ritenute di rischio rilevante

Si riporta di seguito una breve descrizione dei Reati Presupposto relativi a violazioni del diritto d'autore il rischio di commissione dei quali è ravvisabile nello svolgimento dell'attività sociale.

Art. 171 l. 633/41 (comma 1 lett. a bis e 3° comma)

Salvo quanto previsto dall'articolo 171 bis e dall'articolo 171 ter è punito con la multa da € 51,00 a € 2.065,00 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: *"…… **a bis)** mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa".*

Il **3° comma** prevede che: "*La pena è della reclusione fino ad un anno o della multa non inferiore a € 516,00 se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore."*

Art. 171-bis legge 22 aprile 1941, n. 63.

La norma in esame è volta a tutelare il corretto utilizzo dei software e delle banche dati.
Per ciò che concerne i software, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata".
Il reato in ipotesi si configura nel caso in cui chiunque abusivamente duplichi, per trarne profitto, programmi per elaboratore o ai medesimi fini importi, distribuisca, venda, detenga a scopo commerciale o imprenditoriale o conceda in locazione programmi contenuti in supporti non contrassegnati dalla SIAE.
Il fatto è punito anche se la condotta ha ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.
Il secondo comma della stessa norma punisce inoltre chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati ovvero esegue l'estrazione o il reimpiego della banca dati in violazione delle disposizioni di cui alla Legge sul Diritto d'Autore.
Sul piano soggettivo, per la configurabilità del reato è sufficiente lo scopo di lucro, sicché assumono rilevanza penale anche tutti quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico (come nell'ipotesi dello scopo di profitto).
Tale reato potrebbe ad esempio essere commesso nell'interesse della Società qualora venissero utilizzati dei software, per scopi lavorativi, senza essere in possesso della relativa licenza d'uso.

Art. 171-ter, primo comma, b) e c) Legge 22 aprile 1941, n. 633

Il reato si configura allorché un soggetto, per uso non personale: *(i)* abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati [art. 171-ter, primo comma, b)]; *(ii)* detiene o diffonde le opere di cui sopra pur non avendo concorso alla duplicazione o riproduzione [art. 171-ter, primo comma, c)].

- **Aree Sensibili**

I Processi Sensibili individuati sulla base della documentazione relativa al processo di valutazione dei rischi si riferiscono principalmente all'acquisizione e utilizzo di software.

Si richiama quanto indicato nella Matrice dei Rischi allegata al presente Modello.

- **Regole di comportamento**

I Destinatari direttamente coinvolti nelle Aree Sensibili che possono interessare i delitti commessi in violazione del diritto d'autore, devono attenersi alle procedure interne e alla normativa vigente in tema di proprietà intellettuale (e in particolare alla legge n. 633/1941), e di tutela del software e delle banche dati.

- Gestione del software

Nella gestione del software devono essere osservate in particolare le seguenti prescrizioni:

- è vietato l'utilizzo di *software* senza le necessarie autorizzazioni/licenze;
- è vietato l'utilizzo di software al di fuori dei diritti di utilizzazione acquistati;
- la gestione delle autorizzazioni/licenze, e il controllo sull'utilizzo dei relativi *software,* sono di competenza della Funzione IT;
- le funzioni aziendali preposte all'acquisizione di *software* devono ottenere dai propri danti causa garanzie contrattuali in merito *(i)* alla titolarità in capo al cedente dei diritti di utilizzazione economica, *(ii)* alla originalità delle opere e alla inesistenza di violazioni di diritti di terzi;
- sono vietati l'installazione e l'utilizzo di *software* che non siano messi a disposizione dalle funzioni all'uopo autorizzate dalla Società e che non siano funzionali con le mansioni svolte da parte degli utilizzatori;
- sono vietati l'installazione e l'utilizzo, nei sistemi informatici della Società e sui singoli personal computer in dotazione, di software (tipo Peer to Peer) mediante i quali è possibile scambiare file (quale che ne sia il tipo) con altri soggetti all'interno della rete Internet (quali filmati, documenti, canzoni, virus, ecc.) senza alcuna possibilità di controllo da parte della Società;
- è fatto divieto di duplicare e/o diffondere, in qualsiasi forma, programmi, *files* e supporti elettronici (quali a titolo di esempio, CD, DVD, chiavette, ecc.) se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati e nel rispetto delle licenze ottenute.

- Utilizzo opere di terzi

- è fatto espresso divieto di utilizzare, diffondere e/o trasmettere opere di terzi, attraverso siti internet o altri strumenti telematici, in mancanza di accordi contrattuali formalizzati per iscritto con i relativi titolari o in violazione degli accordi medesimi. È, altresì, vietato riprodurre o duplicare i supporti in cui dette opere sono contenute, senza averne acquisiti i relativi diritti.
- il personale non è autorizzato alla riproduzione di supporti sottoposti a licenza d'uso;
- I soggetti coinvolti nei processi sensibili sono tenuti a non consentire ai propri collaboratori utilizzi impropri dei diritti di utilizzazione acquisiti.

- Impiego di data base

I soggetti che si trovassero ad avere la possibilità di gestire banche dati[4] devono osservare le disposizioni di cui agli articoli 64-*quinquies*[5] e 64-*sexies*[6] l.a., e astenersi dall'eseguire l'estrazione o

[4] In base all'art. 102-*bis* si intende per *(i)* costitutore di una banca di dati, chi effettua investimenti rilevanti per la costituzione di una banca di dati o per la sua verifica o la sua presentazione, impegnando, a tal fine, mezzi finanziari, tempo o lavoro; *(ii)* estrazione, il trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma; *(iii)* reimpiego, qualsivoglia forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca di dati mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma. Indipendentemente dalla tutelabilità della banca di dati a norma del diritto d'autore o di altri diritti e senza pregiudizio dei diritti sul contenuto o parti di esso, il costitutore di una banca di dati ha il diritto di vietare le operazioni di estrazione ovvero reimpiego della totalità o di una parte sostanziale della stessa.

[5] In base all'art. 64-*quinquies* spettano all'autore di una banca di dati i diritti esclusivi di eseguire o autorizzare:

a) la riproduzione permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma;
b) la traduzione, l'adattamento, una diversa disposizione e ogni altra modifica;
c) qualsiasi forma di distribuzione al pubblico dell'originale o di copie della banca di dati; la prima vendita di una copia nel territorio dell'Unione europea da parte del titolare del diritto o con il suo consenso esaurisce il diritto di controllare, all'interno dell'Unione stessa, le vendite successive della copia;
d) qualsiasi presentazione, dimostrazione o comunicazione in pubblico, ivi compresa la trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma;
e) qualsiasi riproduzione, distribuzione, comunicazione, presentazione o dimostrazione in pubblico dei risultati delle operazioni di cui alla lettera b).

[6] In base all'art. 64-*sexies* non sono soggette all'autorizzazione dell'autore le attività indicate nell'articolo 64-*quinquies* poste in essere da parte dell'utente legittimo della banca di dati o di una sua copia, se tali attività sono necessarie per l'accesso al contenuto della stessa banca di dati e per il suo normale impiego; se l'utente legittimo è autorizzato ad utilizzare solo una parte della banca di dati, il presente comma si applica unicamente a tale parte. L'articolo in questione precisa inoltre che non sono soggette all'autorizzazione di cui all'articolo 64-*quinquies* da parte del titolare del diritto altre attività, le principali delle quali sono l'accesso o la consultazione della banca dati quando abbia esclusivamente finalità didattiche o di ricerca scientifica, non svolta nell'ambito di un'impresa nonché l'impiego della banca dati per fini di sicurezza pubblica o per effetto di una procedura amministrativa o giurisdizionale.

il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-*bis* e 102-*ter*[7], nonché dal distribuire, vendere o concedere in locazione una banca di dati.

- Utilizzo di marchi, brevetti e diritti di proprietà industriale

L'utilizzo di marchi o brevetti di proprietà di altri, senza le necessarie autorizzazioni, è vietato. Nel caso in cui si debba procedere alla registrazione di un marchio o al deposito di un brevetto si deve preliminarmente verificare, anche con il supporto di consulenti esterni, che non si violino titoli di proprietà industriale di terzi.

- Dubbi

In caso di dubbi in merito a termini e condizioni di utilizzabilità di programmi per elaboratore elettronico o di banche dati di terzi, i Destinatari devono contattare il Servizio Informatico chiedendo le informazioni e i chiarimenti necessari.

Procedure

Devono essere osservati, e si richiamano, i protocolli e la Procedura allegati al presente Modello nonché le altre procedure interne della società.

I controlli dell'Organismo di Vigilanza

Si richiamano i contenuti *(i)* della Parte Generale relativi all'Organismo di Vigilanza e *(ii)* della Parte Speciale Sezione Undicesima.

[7] In base all'art. 102-ter l'utente legittimo della banca di dati messa a disposizione del pubblico non deve arrecare pregiudizio al titolare del diritto e non può eseguire operazioni che siano in contrasto con la normale gestione della banca di dati o che arrechino un ingiustificato pregiudizio al costitutore della banca di dati. Non sono soggette all'autorizzazione del costitutore della banca di dati messa per qualsiasi motivo a disposizione del pubblico le attività di estrazione o reimpiego di parti non sostanziali, valutate in termini qualitativi e quantitativi, del contenuto della banca di dati per qualsivoglia fine effettuate dall'utente legittimo.

PARTE SPECIALE – SEZIONE QUINTA

Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

(Art. 25-septies D.lgs. n. 231/2001)

Le fattispecie di Reati Presupposto riconducibili alla tipologia dei reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla salute e sulla sicurezza del lavoro, ritenute di rischio rilevante

Si riporta di seguito una breve descrizione dei reati contemplati nell'art. 25-septies del D.lgs. 231/2001, introdotto dalla Legge 123/2007 e richiamato nel D.lgs. 9 aprile 2008 n.81.

- **Omicidio colposo (art. 589 c.p.)**

Il reato si configura nel caso in cui si cagioni per colpa la morte di una persona con violazione delle norme per la prevenzione degli infortuni sul lavoro e delle malattie professionali.

- **Lesioni personali colpose gravi o gravissime (art. 590 c.p.)**

Il reato si configura nel caso in cui si cagionino per colpa lesioni personali, gravi o gravissime, con violazione delle norme per la prevenzione degli infortuni sul lavoro e delle malattie professionali.

La lesione è considerata grave (art. 583 c.p., comma 1) nei seguenti casi: *(i)* 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; *(ii)* se il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione è considerata invece gravissima se dal fatto deriva (art. 583 c.p., comma 2): *(i)* una malattia certamente o probabilmente insanabile; *(ii)* la perdita di un senso; *(iii)* 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; *(iv)* la deformazione, ovvero lo sfregio permanente del viso.

Per fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale, il delitto è procedibile d'ufficio.

L'elemento comune ad entrambe fattispecie di reato è la colpa, come definita dall'art. 43 del Codice penale, riferita al verificarsi dell'omicidio e delle lesioni. A tale riguardo, un delitto è da configurarsi come colposo, o contro l'intenzione, quando l'evento, anche se preveduto, non è voluto dall'agente e si verifica a causa di negligenza o imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline.

Tali fattispecie di reato possono realizzarsi ad esempio nel caso in cui, per ottenere un vantaggio (ad esempio un risparmio economico o di tempistiche), non siano stati posti in essere tutti gli accorgimenti e i controlli previsti dalla normativa vigente in materia di sicurezza sul lavoro.

La violazione delle norme in materia di salute e sicurezza sul lavoro può essere invece indifferentemente dolosa o colposa.

- **Tutela della salute e sicurezza sul lavoro**

La Società attribuisce primaria rilevanza, e promuove la diffusione della cultura in materia, alla tutela della salute e sicurezza sul lavoro, anche nei confronti del pubblico che accede ai servizi da essa resi, e intende vincolare i Destinatari al rispetto di tali valori e delle disposizioni legislative e delle autorità preposte in materia.

Il Sistema della Sicurezza di Sardegna IT S.r.l. c.s.u. è definito *(i)* in conformità ai requisiti previsti dall'art. 30 del D.lgs. 81/2008 e s.m.i e *(ii)* secondo gli standard richiesti per la certificazione OHSAS 18001, recepiti.

I Destinatari devono astenersi dal porre in essere, concorrere o dare causa alla realizzazione di comportamenti che possano integrare condotte in violazione della normativa di cui trattasi; devono inoltre attenersi ai principi comportamentali e ai divieti previsti dalle disposizioni del presente Modello e dal Codice Etico.

- **Aree Sensibili**

I Processi Sensibili individuati sulla base della documentazione relativa alla valutazione dei rischi effettuata sono indicati nella Matrice dei Rischi allegata al presente Modello.

- **Regole di comportamento**

  - Destinatari specifici

  Le prescrizioni qui previste si rivolgono ai componenti degli organi sociali di Sardegna IT S.r.l. c.s.u., al Datore di Lavoro, agli eventuali delegati del datore di lavoro ai sensi dell'art. 16 D.lgs. n. 81/2008, al Responsabile del Servizio di Prevenzione e Protezione (RSPP), ai dipendenti e ai Destinatari tutti, ciascuno per quanto di rispettiva competenza, a vario titolo coinvolti nella gestione della salute e della sicurezza sui luoghi di lavoro e nello svolgimento - anche per il tramite di fornitori e consulenti esterni - delle attività relative ai Processi Sensibili in materia.

  - Rispetto della normativa e delle prescrizioni in materia

  I soggetti sopra indicati devono conoscere e rispettare e comunque, per quanto attiene agli organi sociali, far conoscere e far rispettare: *(i)* la normativa, e le istruzioni delle autorità preposte, in tema di salute e sicurezza negli ambienti di lavoro; *(ii)* le regole di cui al Modello, *(iii)* le procedure adottate in tale ambito, *(iv)* le misure di prevenzione e di protezione predisposte a presidio dei rischi connessi alla sicurezza identificati nel Documento di Valutazione dei Rischi ("DVR"), *(v)* il Codice Etico; *(vi)* le linee guida aziendali e le procedure di regolamentazione delle tematiche in materia di salute, igiene e sicurezza sul lavoro.

  L'organizzazione aziendale, come previsto dal D.lgs. 81/2008 e successive integrazioni e modifiche, deve garantire il rispetto delle normative in tema di tutela della salute e dell'integrità fisica dei lavoratori (sicurezza e prevenzione, igiene del lavoro) e di tutela dell'ambiente nonché assicurare in generale un ambiente di lavoro sicuro, sano e idoneo allo svolgimento dell'attività, attraverso:

  1) la valutazione dei rischi, anche da interferenze, per la salute e la sicurezza, sia dei dipendenti e collaboratori, sia del pubblico;
  2) la previsione di opportune garanzie contrattuali nei confronti degli appaltatori, dei prestatori di servizi e dei prestatori d'opera;
  3) la programmazione della prevenzione;
  4) l'eliminazione dei rischi o, ove ciò non sia possibile, la loro riduzione al minimo in relazione alle conoscenze acquisite in base al progresso tecnico;
  5) il rispetto dei principi ergonomici nell'organizzazione del lavoro (posti di lavoro e scelta delle attrezzature) e nella definizione dei metodi di lavoro, per attenuare gli effetti sulla salute del lavoro monotono e di quello ripetitivo;
  6) la limitazione al minimo del numero di lavoratori che sono, o che possono essere, esposti al rischio;
  7) la definizione di priorità delle misure di protezione collettiva, anche nei confronti del pubblico utilizzatore dei servizi resi dalla Società;
  8) la definizione di priorità delle misure di protezione individuale dei propri dipendenti;
  9) il controllo sanitario dei lavoratori, con particolare riguardo ai rischi specifici, ivi compreso l'allontanamento dei lavoratori dall'esposizione al rischio, ove sussistano motivi sanitari inerenti alla loro persona, e l'adibizione, ove possibile, ad altra mansione;
  10) l'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;
  11) la formalizzazione di istruzioni adeguate ai lavoratori;
  12) la definizione di adeguate misure di emergenza da attuare in caso di pronto soccorso, di

lotta antincendio, di evacuazione dei lavoratori e del pubblico dei fruitori dei servizi nonché di pericolo grave e immediato;

13) l'uso di segnali di avvertimento e sicurezza;

14) la regolare manutenzione di automezzi, aree/ambienti, attrezzature e impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti.

Le misure relative alla sicurezza, all'igiene e alla salute durante il lavoro non devono in nessun caso comportare oneri finanziari per i lavoratori.

Nella scelta dei fornitori di beni o servizi 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.

- **Obblighi e divieti dei Destinatari**

I componenti degli organi sociali ed i dipendenti di Sardegna IT S.r.l. c.s.u., compresi il Datore di Lavoro ed il Responsabile del Servizio di Prevenzione e Protezione (RSPP), nello svolgimento - anche per il tramite di fornitori e consulenti esterni - dei compiti ad essi affidati, hanno obbligo di:

- acquisire compiuta conoscenza delle disposizioni normative in materia di igiene, salute e sicurezza sul lavoro, anche attraverso la partecipazione a corsi di formazione istituiti dalla società, tenendo in considerazione anche le specifiche mansioni assegnate;
- rispettare e fare rispettare la normativa e le disposizioni delle autorità, nonché eventuali regolamentazioni di autodisciplina, ed espletare con tempestività gli adempimenti di legge, in tema di igiene e sicurezza del lavoro e ambientale, anche con riferimento alle disposizioni che regolano l'accesso e la presenza negli automezzi della società di terzi estranei alla Società stessa;
- osservare le disposizioni e le istruzioni ricevute ai fini della protezione collettiva e individuale;
- adottare tutte le misure necessarie per la salute e la sicurezza dei lavoratori e del pubblico, nonché le misure per il controllo delle situazioni di rischio in caso di emergenza;
- aggiornare periodicamente le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno una rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;
- sottoporsi ai controlli sanitari previsti;
- nominare i responsabili ed i preposti previsti dalle leggi vigenti assicurando, in generale, un ambiente di lavoro sicuro, sano ed idoneo allo svolgimento dell'attività;
- assegnare gli incarichi di lavoro in relazione alle capacità e alle condizioni dei lavoratori in rapporto alla loro salute e sicurezza;
- dotarsi degli strumenti necessari per evitare che i comportamenti dei singoli possano determinare la responsabilità della persona giuridica;
- utilizzare correttamente gli automezzi, i macchinari, le apparecchiature, gli strumenti di lavoro, le eventuali sostanze pericolose, le altre attrezzature di lavoro, nonché i dispositivi di sicurezza e protezione individuali e collettivi e segnalare immediatamente al Datore di Lavoro eventuali deficienze degli stessi, nonché altre eventuali condizioni di pericolo di cui si venga a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli;
- identificare e delimitare il perimetro delle aree di lavoro interessate alle attività di manutenzione in modo da impedire l'accesso a tali aree da parte di soggetti non autorizzati;
- seguire nella redazione, sottoscrizione ed esecuzione dei contratti le regole di sicurezza diffuse dal Servizio Prevenzione e Protezione;
- attuare le misure di protezione e prevenzione dei rischi sul lavoro che incidono sull'attività lavorativa oggetto di appalto, nonché coordinare gli interventi di protezione e prevenzione al fine di eliminare rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva;
- consentire l'accesso alle zone che espongono a rischi gravi e specifici ai soli lavoratori che abbiano ricevuto al riguardo adeguate istruzioni e specifico addestramento.

Gli appaltatori e in genere i fornitori a qualsiasi titolo e gli installatori di impianti, macchine o altri mezzi tecnici, nonché i progettisti dei luoghi/posti di lavoro, devono, in relazione alla natura del bene fornito o del servizio prestato, garantire il rispetto della normativa sulla sicurezza del lavoro e sulla tutela della salute delle persone.

- **Divieti**

È fatto espresso divieto di:

- rimuovere o modificare senza autorizzazione della direzione aziendale i dispositivi di sicurezza o di segnalazione o di controllo, nonché disattivare o rendere anche parzialmente inefficienti i dispositivi di protezione individuali o collettivi;
- fabbricare, acquistare, noleggiare e utilizzare automezzi, 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.

- **Organizzazione aziendale**

Ai fini del rispetto delle regole e dell'osservanza dei principi, dei divieti e delle prescrizioni elencati nei precedenti paragrafi, i Destinatari devono, nell'ambito del sistema di gestione della sicurezza aziendale, attenersi alle disposizioni di seguito descritte, oltre che alle regole e ai principi generali di comportamento contenuti nella Parte Generale del Modello.

- **Identificazione delle responsabilità**

La Società identifica formalmente, attraverso disposizioni organizzative e deleghe specifiche e a cura dei soggetti individuati dalla normativa rilevante, le responsabilità interne in materia di salute e sicurezza sul lavoro, con particolare riferimento a: Datore di Lavoro, Responsabile e addetti del Servizio di Prevenzione e Protezione, Rappresentanze dei lavoratori per la sicurezza, lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione in caso di pericolo grave e immediato, di salvataggio, di pronto soccorso e, comunque, di gestione dell'emergenza. Tali responsabilità - assegnate attraverso attribuzione formale nell'ambito del rapporto di lavoro o, nel caso di soggetti esterni all'azienda, attraverso idoneo contratto di incarico - devono essere tempestivamente e puntualmente comunicate ai terzi interessati nei casi previsti (es. ASL, Ispettorato del Lavoro, INAIL, ecc.).

- **Servizio di Prevenzione e Protezione**

Il responsabile e gli addetti del Servizio di Prevenzione e Protezione, siano essi interni o esterni, devono: *(i)* avere capacità e requisiti professionali adeguati alla natura dei rischi presenti sul luogo di lavoro e relativi alle attività lavorative; *(ii)* possedere un titolo di studio non inferiore al diploma di istruzione secondaria superiore nonché un attestato di frequenza, con verifica dell'apprendimento, a specifici corsi di formazione adeguati alla natura dei rischi presenti sul luogo di lavoro e relativi alle attività lavorative; *(iii)* essere in numero sufficiente rispetto alle caratteristiche della Società e disporre di mezzi e di tempo adeguati all'espletamento del proprio incarico.

- **Delega di funzioni**

La eventuale delega di funzioni da parte del Datore di Lavoro - ove ritenuta necessaria od opportuna - deve essere conferita ed accettata per iscritto con data certa. Nel processo di attribuzione di deleghe di funzioni devono essere verificati i requisiti di professionalità ed esperienza del delegato, richiesti dalla specifica natura delle funzioni delegate, e devono essere attribuiti al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate, nonché l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate.

- **Preposti**

La Società nomina i preposti, ai quali spetta di vigilare sulla corretta osservanza, da parte di tutti i lavoratori, delle misure e delle procedure di sicurezza adottate dalla Società, segnalando eventuali

carenze o disallineamenti del sistema, nonché comportamenti ad esso contrari.

- **Medico Competente**

Il Datore di Lavoro nomina il Medico competente, che ha il compito di sovrintendere e vigilare sull'osservanza da parte dei singoli lavoratori *(i)* degli obblighi loro derivanti dalla legge, e *(ii)* delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale. Il Medico competente deve possedere i requisiti previsti dalla legge e deve seguire, nello svolgimento dei propri compiti, i principi della medicina del lavoro e del codice etico della Commissione internazionale di salute occupazionale (ICOH).

- **Flussi informativi**

La Società assicura adeguati e tempestivi flussi informativi tra il Datore di Lavoro, il Medico competente e il Servizio di Prevenzione e Protezione in relazione ai processi e ai rischi connessi all'attività della Società, al fine di permettere la collaborazione fra di essi nella valutazione dei rischi, nella programmazione della sorveglianza sanitaria, nella predisposizione dell'attuazione delle misure per la tutela della salute e dell'integrità psico-fisica dei lavoratori, nell'attività di formazione ed informazione nei confronti dei lavoratori e nell'organizzazione del servizio di primo soccorso.

- **Dipendenti**

Tutti i dipendenti devono aver cura della propria sicurezza e salute nonché di quelle del pubblico che fruisce dei servizi di trasporto della Società e di quella delle altre persone che hanno accesso alle strutture della Società, e di osservare tutte le misure di sicurezza, le procedure e le istruzioni aziendali.

- **Misure di prevenzione dei rischi**

In linea generale, la Società adotta le misure più opportune a prevenire il rischio fisico, il rischio psichico e il rischio biologico, sia nei confronti dei propri dipendenti e collaboratori esterni a qualsivoglia titolo, sia nei confronti di coloro che a qualsivoglia titolo utilizzano i servizi della Società.

- **Sistema aziendale di gestione della sicurezza**

Il sistema aziendale di gestione della sicurezza e di tutela dell'igiene del lavoro e della salute dei lavoratori deve essere improntato a garantire l'adempimento di tutti gli obblighi giuridici relativi a:

- esecuzione delle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- attività di informazione e formazione dei lavoratori;
- attività di sorveglianza sanitaria;
- rispetto degli standard tecnico-strutturali di legge relativi ad automezzi, attrezzature, impianti, luoghi di lavoro, agenti fisici, chimici e biologici;
- attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- acquisizione di documentazioni e certificazioni obbligatorie di legge;
- tutela dell'ambiente e smaltimento rifiuti speciali;
- periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Le specifiche procedure e istruzioni fanno parte della documentazione del Sistema di Gestione Integrato e rispondono in particolare agli standard OHSAS 18001.

- **Valutazione dei rischi**

La Società identifica e valuta tutti i rischi per la sicurezza e per la salute dei lavoratori e dei fruitori dei servizi resi, ivi compresi quelli riguardanti gruppi di lavoratori eventualmente esposti a rischi particolari.

La valutazione dei rischi deve essere documentata attraverso l'elaborazione di un *"Documento di valutazione dei rischi ex D.lgs. 81/2008"* (DVR) che contenga i seguenti elementi essenziali e quant'altro prescritto dalla normativa:

a) la valutazione dei rischi per la sicurezza e la salute connessi all'attività della Società, con indicazione dei criteri adottati per la valutazione;

b) l'indicazione delle misure di prevenzione e protezione e dei dispositivi di protezione individuali ritenuti opportuni in conseguenza della suddetta valutazione. I Dispositivi di Protezione Individuale messi a disposizione dei lavoratori devono essere conformi ai requisiti di legge, mantenuti in efficienza, utilizzati per i soli usi previsti e oggetto di specifica attività formativa e informativa; i lavoratori devono utilizzarli in tutti i casi previsti, avendone adeguata cura e senza apportandovi modifiche di propria iniziativa, segnalando qualsiasi difetto o inconveniente in essi rilevato;

c) il programma delle misure ritenute opportune per migliorare nel tempo i livelli di sicurezza;

d) l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché delle funzioni aziendali chiamate a provvedervi, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;

e) l'indicazione del nominativo del Responsabile del Servizio di Prevenzione e Protezione, delle Rappresentanze dei lavoratori per la sicurezza (o di quelle territoriali) e del Medico Competente che ha partecipato alla valutazione del rischio;

f) l'indicazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione ed addestramento.

Il DVR deve avere data certa, deve essere approvato dal Datore di Lavoro, dal RSPP e dal Medico competente, previa consultazione delle Rappresentanze dei lavoratori per la sicurezza (a cui deve esserne fornita copia), e deve essere custodito presso l'unità produttiva di riferimento.

La valutazione del rischio deve essere condotta secondo metodi e criteri trasparenti, esaustivi e di agevole utilizzo.

In caso di mutamenti del processo produttivo e/o dell'organizzazione del lavoro significativi ai fini della tutela della salute e sicurezza dei lavoratori, e/o in relazione al grado di evoluzione delle tecniche di prevenzione e protezione, e/o a seguito di infortuni significativi, e/o quando i risultati della sorveglianza sanitaria ne postulino la necessità, il DVR deve essere tempestivamente aggiornato con l'introduzione di misure idonee a disciplinare la nuova situazione verificatasi.

- **Situazioni di emergenza**

  - <u>Piano di sicurezza e di gestione delle emergenze</u>

Devono essere adottate, a cura del Servizio di Protezione e Prevenzione, misure per fronteggiare situazioni di emergenza, con elaborazione, aggiornamento periodico ed esercitazioni programmate, del Piano di sicurezza e di gestione dell'emergenza, contenente istruzioni e procedure da osservarsi nei casi di *(i)* incendio, *(ii)* evacuazione degli insediamenti e dei mezzi di trasporto, *(iii)* infortunio e malore, *(iv)* pronto soccorso.

Il Piano deve contenere i seguenti elementi essenziali:

- ✓ descrizione dei luoghi di lavoro e valutazione del rischio incendio,
- ✓ disposizioni per l'organizzazione degli interventi di emergenza (personale incaricato e relativi compiti),
- ✓ un piano generale di emergenza.

La Società assicura tempestività degli interventi dei servizi pubblici competenti in materia di pronto soccorso, salvataggio, lotta antincendio e gestione dell'emergenza.

Una sintesi del Piano di Emergenza, nonché le procedure e le istruzioni rilevanti, devono essere distribuite e/o messe a disposizione di tutti i lavoratori interessati.

- Rischio di incendio

Per quanto attiene in particolare il rischio incendio deve essere predisposto e tempestivamente aggiornamento a cura del Servizio di Protezione e Prevenzione, ove necessario in relazione a variazioni di rischio, un Documento di Valutazione dei rischi di incendio nei luoghi di lavoro, ai sensi del D.M. 10 marzo 1998, che contenga:

- ✓ la valutazione dei rischi di incendio nei luoghi di lavoro, con illustrazione dei pericoli identificati e indicazione dei criteri e della metodologia adottata;
- ✓ l'ubicazione dell'unità produttiva e l'identificazione del tipo di edificio e degli impianti a rischio incendio, con la specificazione delle caratteristiche costruttive, delle vie di esodo, dei presidi antincendio;
- ✓ l'identificazione dei dipendenti e delle altre persone esposte al rischio di incendio, le misure di protezione antincendio adottate, con particolare riferimento a: *(i)* l'adozione di attrezzature, impianti e dispositivi antincendio adeguati, con la programmazione delle necessarie verifiche e manutenzioni; *(ii)* la dotazione di adeguate misure di primo soccorso; *(iii)* l'identificazione di una o più squadre di pronto intervento, costituite da un numero adeguato di persone debitamente formate in materia di antincendio, pronto soccorso ed evacuazione; *(iv)* la definizione del piano di evacuazione dei luoghi e la effettuazione e documentazione di periodiche prove di esodo; *(v)* la formazione del personale incaricato; e *(vi)* l'informativa al personale interessato.

Il documento deve essere approvato dal Datore di Lavoro e dal RSPP e custodito presso l'unità produttiva di riferimento.

Per tutti i luoghi di lavoro devono essere ottenuti, e ove del caso adeguati, e conservati i Certificati di Prevenzione Incendi e le certificazioni relative agli impianti (quali centrale termica, ascensori, impianti elettrici e ogni altro impianto) secondo quanto previsto da norme di legge; inoltre devono essere

conservati i verbali delle relative verifiche periodiche e le eventuali segnalazioni di conformità agli enti competenti.

- **Budget**

La Società si impegna, nell'ambito dei propri budget, ad attenersi alle tecnologie adeguate al raggiungimento degli obbiettivi sopra delineati e ad astenersi dall'assumere decisioni nel campo della sicurezza, salute e igiene sul lavoro riferendosi esclusivamente a una politica di taglio dei costi e degli investimenti.

La Società deve comunicare all'ODV il budget stanziato per la sicurezza.

- **Svolgimento dei servizi per il pubblico**

Nello svolgimento dei servizi per il pubblico devono essere osservate tutte le precauzioni necessarie ed opportune ai fini della tutela dell'integrità fisica sia del pubblico sia degli addetti. Lo stesso deve essere osservato per quanto attiene i trasferimenti interni ed esterni dei dipendenti, sia con mezzi aziendali sia con mezzi propri.

- **Affidamento di appalti (DUVRI)**

Adeguate misure di sicurezza, con la nomina di un responsabile della sicurezza, devono essere assunte anche in relazione all'affidamento di appalti d'opera o di servizi, sia nella fase di progettazione sia nella fase di esecuzione. È inoltre richiesto, nei casi di apertura di cantieri, il rispetto della specifica normativa riguardante i cantieri temporanei (Titolo IV del d.lgs. 81/2008) e l'adozione di tutte le misure ivi previste.

In particolare, deve per ciascun appalto essere predisposto un Documento di Valutazione dei Rischi da Interferenze (DUVRI), ma solo nei casi in cui vi siano più imprese a svolgere attività lavorativa contestualmente e non,

La predisposizione del DUVRI viene effettuata dal Responsabile del settore con il supporto dell'RSPP, valutando tutti i fattori di rischio inerenti all'attività svolta. Una volta terminata la stesura del DUVRI, il Resposabile trasmette al Datore di Lavoro una comunicazione in cui dichiara di aver analizzato i contenuti del DUVRI, confermandone la completezza e la corretta redazione. Infine, la Società invia il

DUVRI a mezzo raccomandata a.r. al fornitore di servizi interessato, il quale a sua volta ne prenderà visione e lo restituirà sottoscritto a Sardegna IT S.r.l. c.s.u., sempre mediante raccomandata a.r.

- **Sorveglianza sanitaria**

La sorveglianza sanitaria è svolta dal Medico competente attraverso protocolli sanitari definiti in funzione dei rischi specifici e considerando gli indirizzi scientifici più avanzati; la stessa deve essere effettuata in conformità dalla normativa vigente, alle direttive europee, nonché alle indicazioni fornite dalla Commissione consultiva, e qualora il lavoratore ne faccia richiesta e la stessa sia ritenuta dal Medico competente correlata ai rischi lavorativi.

In particolare, la sorveglianza sanitaria comprende: *(i)* visita medica preventiva al momento dell'inserimenti nell'azienda ai fini di valutare l'idoneità alla mansione, *(ii)* visita medica periodica, *(iii)* visita medica su richiesta del lavoratore al fine di esprimere il giudizio di idoneità alla mansione specifica, *(iv)* visita medica in occasione del cambio della mansione onde verificare l'idoneità alla nuova mansione, *(v)* visita medica alla cessazione del rapporto di lavoro, nei casi previsti dalla normativa vigente. Per ciascun lavoratore sottoposto a sorveglianza sanitaria deve essere istituita e tempestivamente aggiornata una cartella sanitaria e di rischio.

Le attività di monitoraggio e sorveglianza del Piano di sorveglianza sanitaria devono essere documentate attraverso apposita Relazione Sanitaria, predisposta dal Medico competente con cadenza annuale e indirizzata al Servizio di Prevenzione e Protezione e al Datore di Lavoro.

- **Infortuni**

La Società deve predisporre un report sul quale annota gli infortuni sul lavoro del personale che comportano un'assenza di almeno un giorno.

L'acquisizione e trasmissione dei dati informativi relativi agli infortuni devono essere effettuate sulla base e nel rispetto di specifiche procedure interne formalizzate.

Devono essere anche esaminate ai fini di eventuali interventi organizzativi, le situazioni di c.d. "quasi infortuni", vale a dire delle situazioni nelle quali, per carenze organizzative, avrebbe potuto verificarsi un infortunio.

- **Informazione e formazione**
  - Informazione

    La Società attua un programma di informazione dei dipendenti e collaboratori in materia tutela dell'igiene e della sicurezza sul lavoro, relativamente a: rischi per la sicurezza e la salute connessi all'attività aziendale; misure e attività di prevenzione e protezione adottate; rischi specifici cui si è esposti in relazione all'attività svolta, pericoli connessi all'uso delle sostanze e dei preparati pericolosi sulla base delle schede dei dati di sicurezza previsti dalla normativa vigente e dalle norme di buona tecnica; misure ed attività che riguardano il pronto soccorso, la lotta antincendio, l'evacuazione dei lavoratori; nomina del RSPP e del Medico competente; nominativi dei lavoratori incaricati per la sicurezza; legislazione di riferimento applicabile; *policy* e procedure aziendali in materia di salute e sicurezza sul lavoro.

  - Formazione

    Per i lavoratori e collaboratori che rivestono specifiche responsabilità in materia di igiene e sicurezza sul lavoro viene attuato uno specifico programma di formazione e aggiornamento, differenziato in base alle mansioni affidate e ai differenti profili di rischio di appartenenza dell'azienda. Lo svolgimento e la partecipazione ai corsi in materia di salute, igiene e sicurezza sul lavoro devono essere monitorati e adeguatamente documentati, anche attraverso l'archiviazione e la custodia dei relativi programmi e attestati di frequenza.

- **Rappresentanze dei lavoratori**

Alle Rappresentanze per la sicurezza è garantito il libero accesso alle informazioni e alla documentazione prescritta dalla normativa vigente, nel rispetto dei vincoli in termini di riservatezza e confidenzialità delle informazioni stesse.

- **Segnalazione di nuovi rischi**

La Società incoraggia il personale dipendente ad effettuare segnalazioni di nuovi rischi e pericoli di cui la Società assicura la raccolta e la conseguente trattazione. Inoltre, la Società raccoglie e tratta le segnalazioni da parte degli enti di controllo sino alla risoluzione della problematica denunciata.

- **Sanzioni**

La violazione delle prescrizioni normative e delle regole aziendali in materia di tutela della salute e sicurezza sui luoghi di lavoro costituiscono violazione del Modello e, pertanto, illecito disciplinare sanzionabile secondo quanto previsto nella Parte Generale.

Procedure

Devono essere osservati, e si richiamano, i protocolli e la procedura allegati al presente Modello nonché le altre procedure interne della società.

I controlli dell'Organismo di Vigilanza

Si richiamano i contenuti *(i)* della Parte Generale relativi all'Organismo di Vigilanza e *(ii)* della Parte Speciale Sezione Undicesima.

PARTE SPECIALE - SEZIONE SESTA

Delitti informatici e trattamento illecito di dati

(Art. 24-bis D.lgs. 231/2001)

Le fattispecie di Reati Presupposto riconducibili alla tipologia dei reati informatici e trattamento illecito di dati ritenute di rischio rilevante

Si riporta qui di seguito una breve descrizione dei Reati Presupposto di questa Sezione Settima della Parte Speciale.

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

Il reato si configura nel caso di falsità riguardanti un documento informatico pubblico o privato avente efficacia probatoria.

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale (cfr. Capo III, Titolo VII, Libro II), 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 pubblico o privato e avente efficacia probatoria.

In particolare, si precisa che si ha "falsità materiale" quando un documento non proviene dalla persona che risulta essere il mittente o da chi risulta dalla firma (contraffazione) ovvero quando il documento è artefatto (e, quindi, alterato) per mezzo di aggiunte o cancellazioni successive alla sua formazione.

Si ha, invece, "falsità ideologica" quando un documento non è veritiero nel senso che, pur non essendo né contraffatto né alterato, contiene dichiarazioni non vere.

I Documenti Informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

A titolo esemplificativo, integra il delitto di falsità in Documenti Informatici la condotta di chi falsifichi documenti informatici aziendali contenenti gli importi dovuti dall'ente alla Pubblica Amministrazione (ad esempio in relazione al pagamento dei contributi previdenziali per i Dipendenti), la falsificazione di comunicati stampa o altra forma di comunicazione dovuta alle Autorità di Vigilanza come la Consob.

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

Il reato si configura quando un soggetto si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

A tal riguardo si sottolinea come il legislatore abbia inteso punire l'accesso abusivo ad un sistema informatico o telematico tout court, e dunque anche quando ad esempio all'accesso non segua un vero e proprio danneggiamento di dati: si pensi all'ipotesi in cui un soggetto acceda abusivamente ad un sistema informatico al fine di eseguire unicamente una copia (accesso abusivo in copiatura), o di visualizzare alcune informazioni (accesso abusivo in sola lettura).

La suddetta fattispecie delittuosa si realizza altresì nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema, nonché, secondo il prevalente orientamento giurisprudenziale, qualora il medesimo abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Il delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi informatici di proprietà di società concorrenti nell'ambito di una gara di appalto al fine di conoscere l'entità delle offerte presentate da queste ultime.

Il reato è perseguibile a querela della persona offesa, fatto salvo il configurarsi di circostanze aggravanti, quali l'utilizzo di violenza su cose o persone o la distruzione o il danneggiamento di dati, informazioni o programmi quale conseguenza dell'accesso abusivo.

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

Il reato si configura 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 ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Tale reato si realizza qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo.

Il legislatore ha introdotto tale reato al fine di prevenire le ipotesi di accesso abusivo a sistemi informatici.

Per mezzo dell'art. 615-quater cod. pen., sono pertanto 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 (quali badge o smart card).

Tale fattispecie si configura sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (ad esempio, un operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.

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

Il reato potrebbe astrattamente configurarsi nell'ipotesi in cui un dipendente della società riesca a procurarsi illecitamente la Password per accedere al sistema informatico della Procura presso cui siano registrati documenti informatici aventi efficacia probatoria in relazione ad un procedimento in cui sia coinvolta la società medesima, a prescindere dall'accesso abusivo a tale sistema informatico.

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.)

Il reato si configura, salvo che il fatto costituisca più grave reato, 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 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 al soddisfacimento di un interesse di natura pubblica.

Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria registrati presso enti pubblici (es. polizia giudiziaria) relativi ad un procedimento penale a carico della società.

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

Il reato si configura quando la condotta di cui all'articolo 635-quater è diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Aree Sensibili

I Processi Sensibili individuati sulla base della documentazione relativa alla valutazione dei rischi effettuata sono indicati nella Matrice dei Rischi allegata al presente Modello.

Regole di comportamento

- Destinatari

  Le regole di comportamento che seguono si applicano ai Destinatari che, a qualunque titolo, sono incaricati della gestione e manutenzione dei server, delle banche dati, delle applicazioni, dei client e delle reti di telecomunicazione, nonché a tutti coloro che abbiano accesso al sistema informativo

aziendale ed in particolare a coloro che abbiano avuto assegnate password e chiavi di accesso.

- Rispetto della normativa e delle prescrizioni in materia

  I Destinatari di cui sopra, ciascuno per quanto di rispettiva competenza, devono conoscere e rispettare e comunque, per quanto attiene agli organi sociali, far conoscere e far rispettare: *(i)* la normativa, e le istruzioni delle autorità preposte, in tema di sistemi informativi e trattamento dati; *(ii)* le regole di cui al Modello; *(iii)* il Codice Etico; *(iv)* le procedure.

  L'organizzazione aziendale deve garantire il rispetto delle normative in materia.

- Obblighi e divieti di carattere generale

  I Destinatari:

  - non possono utilizzare connessioni alternative rispetto a quelle fornite dalla Società;
  - possono accedere al sistema informativo unicamente attraverso i codici di identificazione assegnati univocamente;
  - devono astenersi da qualsiasi condotta che possa compromettere la riservatezza e integrità delle informazioni e dei dati di Sardegna IT S.r.l. c.s.u. e dei terzi;
  - devono astenersi da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informatico aziendale;
  - devono conservare i codici identificativi, con divieto di comunicarli a terzi;
  - non devono installare programmi senza le autorizzazioni previste nelle procedure interne;
  - non devono 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;
  - devono rispettare la proprietà e titolarità dei sistemi informatici altrui.

- Misure minime di sicurezza

  Gli amministratori di sistema[8] devono porre in essere misure idonee a prevenire fenomeni di *hackeraggio*, quali in via esemplificativa, i necessari firewall che impediscano l'accesso dall'esterno. Gli amministratori di sistema sono muniti di proprie credenziali di autenticazione.

  La Società, con il supporto degli amministratori di sistema, deve predisporre le seguenti misure minime di sicurezza:

  - accesso alle informazioni che risiedono sui server e sulle banche dati aziendali controllato da modelli, procedure e strumenti di autenticazione, con dotazione al personale dipendente di univoche credenziali di accesso ai client;
  - adozione e gestione delle credenziali di accesso mediante specifiche procedure;
  - accesso alle applicazioni garantito attraverso strumenti di autorizzazione;
  - verifica periodica dell'individuazione dell'ambito del trattamento dati consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
  - aggiornamento periodico dei server e dei PC (anche portatili) sulla base delle specifiche necessità;
  - protezione dei dispositivi elettronici e dei dati contro trattamenti illeciti di dati, accessi non consentiti e determinati programmi informatici;
  - adozione di procedure per la custodia di copie di sicurezza e per il ripristino della disponibilità dei dati e dei sistemi;

[8] In assenza di definizioni normative e tecniche condivise, l'amministratore di sistema viene definito nel Provvedimento del Garante Privacy del 27 novembre 2008 come "una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (*Enterprise resource planning*) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali".

- impossibilità di replicare abusivamente password e codici di accesso a sistemi informatici o telematici; le password devono essere custodite in apposito contenitore sottoposto anch'esso a password;
- qualsiasi accesso al sistema e uscita dallo stesso da parte dell'amministratore di sistema deve essere tracciato, anche al fine di consentire la rilevazione di un'eventuale alterazione del sistema da parte degli utenti, nel rispetto della normativa in materia di Privacy;
- agli amministratori di sistema è fatto divieto di operare al di fuori dei propri compiti senza l'autorizzazione dell'utente interessato;
- i dati di rete replicati su personal computer devono essere resi disponibili solo agli utenti autorizzati;
- protezione dei dispositivi di networking mediante adeguati strumenti di limitazione degli accessi dall'esterno (firewall e proxy);
- collocazione dei dispositivi di networking in aree dedicate e protette al fine di renderli accessibili al solo personale autorizzato;
- protezione dei server, dei PC e di altri eventuali dispositivi elettronici (quali laptop, telefoni mobili e simili) con programmi antivirus, aggiornati in modo automatico contro il rischio di intrusione;
- accesso ai server limitato al solo personale autorizzato al fine di garantire la sicurezza fisica dei dati ivi contenuti e gestiti;
- protezione dei server mediante dispositivi adeguati a prevenire comportamenti anomali.
- duplicazione dei server.

La Società adotterà un Regolamento volto in via principale ad assicurare e disciplinare la regolamentazione del sistema di gestione e di monitoraggio della protezione e dell'accesso, ai vari livelli funzionali, ai sistemi informatici e telematici aziendali. Tutti i Destinatari devono osservare le disposizioni del Regolamento sopra menzionato.

- Tracciabilità

  La Società deve seguire regole che garantiscano il rispetto della normativa in materia nonché la tracciabilità e trasparenza delle scelte operate, mantenendo a disposizione dell'ODV tutta la documentazione di supporto.

- Comunicazini ai fini della sicurezza nazionale cibernetica

  Le comunicazioni di cui trattasi (in quando concernenti dati, informazioni o elementi di fatto rilevanti ai fini della sicurezza cibernetica nazionale) devono essere rese dall'Amministratore delegato della Società, o persona da lui espressamente delegata per iscritto, previa verifica e approvazione da parte del responsabile IT. Nel caso in cui il delegato sia il responsabile IT, le comunicazioni dovranno comunque essere approvate dall'Amministratore delegato.

  Le comunicazioni dovrenno in ogni caso essere rese entro i termini prescritti e non è consentita la loro omissione.

Coordinamento con le disposizioni del GDPR e del D.lgs. 10/08/2018 n° 101 "armonizzazione del Codice della privacy alla normativa europea"

La Società è consapevole che la matrice delle misure del Modello 231 che attengono la prevenzione di condotte/reato che possano verificarsi nell'interesse o a vantaggio dell'ente, commesse da soggetti interni alla rete, si incrocia con la matrice delle misure del separato e diverso modello per l'attuazione del GDPR e del D.lgs. 10/08/2018 n° 101 ("armonizzazione del Codice della privacy alla normativa europea") che attengono la protezione della sicurezza dei dati a prescindere dal fatto che la violazione avvenga da soggetti interni o esterni. È infatti da ritenersi pacifico che la commissione di reati informatici possa comportare il rischio di una violazione della sicurezza dei dati che produca «la divulgazione non autorizzata o l'accesso ai dati personali», e ciò indifferentemente dal fatto che la violazione si realizzi accidentalmente o in modo illecito. In ogni caso la violazione può comportare pesanti conseguenze sanzionatorie di natura economica, e di risarcimento danni, nei confronti della Società.

Con riferimento a quanto sopra la Società provvede a un coordinamento funzionale tra i due sistemi organizzativi e di prevenzione (231 e GDPR), tenuto conto (i) del catalogo dei reati presupposto informatici,

(ii) delle altre fattispecie di reato la cui condotta realizzativa si avvale dell'utilizzo dei sistemi informatici [quali ad es. la frode informatica

(art. 640-ter c.c.), talune fattispecie di reato societario (ex art. 25-ter), taluni delitti in materia di violazione del diritto d'autore (ex art. 25-novies)] e (iii) dell'impatto dell'informatica anche sulla gestione del whistleblowing ex l.179/2017.

In quest'ottica i Titolari del trattamento terranno conto del Modello 231 nella redazione del Registro di trattamento dei dati, ma anche l'ODV dovrà acquisire i registri del trattamento dati e verificare che le due matrici di rischio non siano in contrapposizione l'una con l'altra, dando diverse interpretazioni alla stessa funzione di protezione, coordinandosi in merito con il Responsabile della protezione dei dati (DPO).

Procedure

Devono essere osservati, e si richiamano, i protocolli e la procedura allegati al presente Modello nonché le procedure interne della società.

I controlli dell'Organismo di Vigilanza

Si richiamano i contenuti *(i)* della Parte Generale relativi all'Organismo di Vigilanza e *(ii)* della Parte Speciale Sezione Undicesima

PARTE SPECIALE - SEZIONE SETTIMA

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

(Art. 25-decies D.lgs. n. 231/2001)

La fattispecie di reato-presupposto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies D.lgs. 231/2001)

Si riporta di seguito una breve descrizione del Reato Presupposto di cui trattasi.

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)

Il reato si configura quando, con uso di violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, si induce un soggetto a non rendere dichiarazioni o a rendere dichiarazioni mendaci davanti all'autorità giudiziaria, dichiarazioni utilizzabili in un procedimento penale, quando questo ha la facoltà di non rispondere.

Aree Sensibili

I Processi Sensibili individuati sulla base della documentazione relativa alla valutazione dei rischi effettuata sono indicati nella Matrice dei Rischi allegata al presente Modello.

Regole di comportamento

- Principi Generali

  In linea generale, i destinatari del Modello devono attenersi al principio di non interferire con il corretto andamento dell'amministrazione della giustizia, astenendosi dal fare, o far fare, pressioni su testimoni; ove a conoscenza di intendimenti di terzi in tal senso, devono attivarsi per cercare di dissuadere da tali comportamenti.

  Il principio sopra specificato si applica ai componenti degli organi sociali e a tutti i dipendenti di Sardegna IT S.r.l. c.s.u.

  È fatto divieto 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.

  La Società promuove il rispetto del Codice Etico e della verità e trasparenza della documentazione utilizzata, in ogni circostanza.

- Obblighi

  Ai Destinatari che abbiano rapporti con l'autorità giudiziaria è richiesto di:

  - evadere con tempestività, correttezza e buona fede tutte le richieste provenienti dagli organi di polizia giudiziaria e dall'autorità giudiziaria inquirente e giudicante, fornendo tutte le informazioni, i dati e le notizie eventualmente utili;
  - mantenere, nei confronti degli organi di polizia giudiziaria e dell'autorità giudiziaria un comportamento disponibile e collaborativo in qualsiasi situazione.

- Divieti

  I Destinatari che abbiano rapporti con l'autorità giudiziaria devono astenersi dal ricorrere alla forza fisica, a minacce o all'intimidazione oppure promettere, offrire o concedere un'indebita utilità per indurre chi deve testimoniare o rendere dichiarazioni nell'ambito di un procedimento penale a non rendere dichiarazioni o a rendere false dichiarazioni all'autorità giudiziaria. con l'intento di ottenere una pronuncia favorevole per la Società o determinare il conseguimento di altro genere di vantaggio.

Procedure specifiche

Le controversie davanti all'Autorità Giudiziaria devono essere tracciabili e deve essere individuata la responsabilità della relativa gestione.

Devono essere osservati, e si richiamano, i protocolli e la Procedura allegati al presente Modello nonché le altre procedure interne della società.

I controlli dell'Organismo di Vigilanza

Si richiamano i contenuti *(i)* della Parte Generale relativi all'Organismo di Vigilanza, *(ii)* della Parte Speciale Sezione Undicesima.

PARTE SPECIALE – SEZIONE OTTAVA

Reati concernenti l'impiego di lavoratori in violazione di particolari norme di legge:

Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

(Art. 25-duodecies D.lgs. n. 231/2001)

Intermediazione illecita e sfruttamento del lavoro

(Art. 25-quinquies D.lgs. n. 231/2001)

Le fattispecie di Reati Presupposto di impiego di lavoratori in violazione di particolari norme di legge ritenute di rischio rilevante.

Si riporta di seguito una breve descrizione dei Reati Presupposto di cui trattasi.

- **Impiego di lavoratori stranieri il cui soggiorno è irregolare (Articolo 22, comma 12 e 12-bis, D.lgs. 25 luglio 1998, n. 286)**

Il reato si configura quando il datore di lavoro occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto - e del quale non sia stato chiesto, nei termini di legge, il rinnovo -, revocato o annullato.

Ai fini della punibilità dell'ente occorre la sussistenza di una delle aggravanti di cui appresso, che comportano un aumento di pena: *(i)* che i lavoratori occupati siano in numero superiore a tre; *(ii)* che i lavoratori occupati siano minori in età non lavorativa; *(iii)* che i lavoratori occupati siano sottoposti a condizioni lavorative di particolare sfruttamento (di cui al terzo comma dell'articolo 603-*bis* del codice penale). Le condizioni di particolare sfruttamento sono, oltre a quelle sopra riportate ai punti *(i)* e *(ii)*, l'aver commesso il fatto esponendo i lavoratori intermediati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

- **Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)**

Il reato si configura nei confronti di chiunque:

(i) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;

(ii) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

Ai fini della sussistenza del reato costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:

a) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;

b) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;

c) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;

d) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

Costituiscono aggravante specifica e comportano l'aumento della pena da un terzo alla metà *(i) il fatto che i lavoratori occupati siano in numero superiore a tre; (ii) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa; (iii) l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo*, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

Processi Sensibili

I Processi Sensibili individuati sulla base della valutazione dei rischi si riferiscono principalmente al ricorso di manodopera attraverso agenzie interinali o società cooperative, nonché all'impiego di manodopera da

parte degli appaltatori.

La Società ha proceduto all'aggiornamento della Matrice dei Rischi.

I soggetti intervistati ritengono che il verificarsi del reato di cui trattasi in caso di assunzione diretta da parte della Società sia nella sostanza impossibile.

Regole di comportamento

I Destinatari dovranno osservare la normativa in materia di impiego di cittadini di paesi terzi, nonché attenersi ai Principi Generali e alle Regole contenuti nella Parte Generale del Modello, nel Codice Etico, nelle procedure specifiche e nei protocolli del presente Modello.

È fatto divieto 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.

Condizioni per l'impiego

Si precisa che *impiego* va inteso come effettività della prestazione lavorativa, e quindi utilizzo in concreto delle prestazioni (e non assunzione).

L'impiego di manodopera, sia assunta direttamente da parte della Società, sia attraverso il ricorso ad agenzie interinali o a società cooperative, ove si tratti di cittadini di paesi terzi, deve riguardare lavoratori muniti del permesso di soggiorno, ovvero del cui permesso di soggiorno sia stato chiesto, nei termini di legge, il rinnovo; ovvero il cui permesso di soggiorno non sia stato revocato o annullato.

Le medesime regole valgono per il personale degli appaltatori che opera presso unità della Società.

Contratti con agenzie interinali o cooperative

I contratti con agenzie di lavoro interinale o con cooperative, così come i contratti con gli appaltatori, devono contenere specifiche garanzie.

Inoltre nei suddetti contratti deve essere contenuta apposita dichiarazione dei contraenti:

a) di essere a conoscenza della normativa di cui al D.lgs. 231/2001 e delle sue implicazioni per la Società,

b) di essere a conoscenza della normativa di cui al D.lgs. 25 luglio 1998, n. 286, con particolare riferimento all'art. 22;

c) di essere a conoscenza dell'art. 603-bis c.p. come modificato dalla legge 29 ottobre 2016 n. 199;

d) di impegno a rispettare le disposizioni e i divieti specificati nella presente Parte Speciale;

e) di impegno ad astenersi dal compiere attività che possano configurare alcuno dei Reati Presupposto o che comunque si pongano in contrasto con lo stesso.

Per il resto si rimanda alle disposizioni delle Parte Speciale Sezione Undicesima.

Procedure

Devono essere osservati, e si richiamano, i protocolli e la Procedura allegati al presente Modello nonché le altre procedure interne della società.

I controlli dell'Organismo di Vigilanza

Si richiamano i contenuti *(i)* della Parte Generale relativi all'Organismo di Vigilanza e *(ii)* della Parte Speciale Sezione Undicesima.

PARTE SPECIALE – SEZIONE NONA

Reati tributari di cui al decreto legislativo 10 marzo 2000, n. 74 "Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della legge 25 giugno 1999, n. 205".

(Art. 25-quinquesdecies)

Premessa

Questa Sezione Decima della Parte Speciale si riferisce ai comportamenti dei Destinatari coinvolti nei Processi Sensibili concernenti i Reati Presupposto tributari: si tratta di taluni reati, appresso singolarmente considerati in dettaglio, che non esauriscono la categoria dei reati in tale materia.

I reati di cui trattasi sono stati introdotti nel catalogo dei reati di cui al Decreto 231 mediante inserimento in detto decreto dell'art. 25-*quinquiesdecies* (Reati tributari), che attribuisce all'ente/società una responsabilità diretta per la commissione, nell'interesse o a vantaggio dell'ente/società stesso, di alcuni reati tributari contemplati nel decreto legislativo 10 marzo 2000, n. 74 "Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della legge 25 giugno 1999, n. 205".

Fattispecie dei Reati Presupposto tributari ritenute di rischio rilevante (art. 25-*quinquiesdecies*)

Definizioni

Per una appropriata lettura e comprensione delle disposizioni di legge di cui appresso va premesso che, ai fini della normativa tributaria di cui al citato D.lgs. n.74/2000), si applicano le seguenti definizioni di carattere generale applicabili a tutti i Reati Presupposto tributari:

a) per "fatture o altri documenti per operazioni inesistenti" si intendono le fatture o gli altri documenti aventi rilievo probatorio analogo in base alle norme tributarie, *(i)* emessi a fronte di operazioni non realmente effettuate in tutto o in parte o *(ii)* che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero *(iii)* che riferiscono l'operazione a soggetti diversi da quelli effettivi;

b) per "elementi attivi o passivi" si intendono *(i)* le componenti, espresse in cifra, che concorrono, in senso positivo o negativo, alla determinazione del reddito o delle basi imponibili rilevanti ai fini dell'applicazione delle imposte sui redditi o sul valore aggiunto e *(ii)* le componenti che incidono sulla determinazione dell'imposta dovuta;

c) per "dichiarazioni" si intendono anche le dichiarazioni presentate in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche o di sostituto d'imposta, nei casi previsti dalla legge;

d) il "fine di evadere le imposte" e il "fine di consentire a terzi l'evasione" si intendono comprensivi, rispettivamente, anche *(i)* del fine di conseguire un indebito rimborso o il riconoscimento di un inesistente credito d'imposta, e *(ii)* del fine di consentirli a terzi;

e) riguardo ai fatti commessi da chi agisce in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche, il "fine di evadere le imposte" ed il "fine di sottrarsi al pagamento" si intendono riferiti alla società, all'ente o alla persona fisica per conto della quale si agisce;

f) per "imposta evasa" si intende la differenza tra l'imposta effettivamente dovuta e quella indicata nella dichiarazione, ovvero l'intera imposta dovuta nel caso di omessa dichiarazione, al netto delle somme versate dal contribuente o da terzi a titolo di acconto, di ritenuta o comunque in pagamento di detta imposta prima della presentazione della dichiarazione o della scadenza del relativo termine; non si considera imposta evasa quella teorica e non effettivamente dovuta collegata a una rettifica in diminuzione di perdite dell'esercizio o di perdite pregresse spettanti e utilizzabili;

g) le soglie di punibilità riferite all'imposta evasa si intendono estese anche all'ammontare dell'indebito rimborso richiesto o dell'inesistente credito di imposta esposto nella dichiarazione;

h) per "operazioni simulate oggettivamente o soggettivamente" si intendono *(i)* le operazioni

apparenti, diverse da quelle disciplinate dall'articolo 10-*bis* della legge 27 luglio 2000, n. 212, poste in essere con la volontà di non realizzarle in tutto o in parte ovvero *(ii)* le operazioni riferite a soggetti fittiziamente interposti;

i) per "mezzi fraudolenti" si intendono condotte artificiose attive nonché quelle omissive realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà.

Aumenti delle sanzioni a carico dell'ente/società

Sempre in linea generale, va altresì premesso che le sanzioni pecuniarie appresso indicate sono aumentate di un terzo qualora, a seguito alla commissione dei delitti di cui trattasi (indicati nel comma 1 dell'art. 25-*quinquiesdecies* e appresso considerati in dettaglio), l'ente abbia conseguito un profitto di rilevante entità.

Sanzioni interdittive

Nei casi previsti dai commi 1 e 2 dell'art. 25-quinquiesdecies si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e).

Fattispecie di Reati Presupposto tributari

- **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art. 2, comma 1 e comma 2-bis, D.lgs. 10 marzo 2000, n. 74)**

La fattispecie di reato si configura a carico di coloro che, al fine di evadere le imposte sui redditi o sul valore aggiunto, indicano, in una delle dichiarazioni relative a dette imposte, elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti.

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.

- **Dichiarazione fraudolenta mediante altri artifici (art. 3 D.lgs. 10 marzo 2000, n. 74)**

La fattispecie di reato si configura allorché, fuori dai casi previsti dall'articolo 2 (di cui sopra), al fine di evadere le imposte sui redditi o sul valore aggiunto, il soggetto autore del reato - *(i)* compiendo operazioni simulate oggettivamente o soggettivamente ovvero *(ii)* avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria - indichi in una delle dichiarazioni relative a dette imposte *(i)* elementi attivi per un ammontare inferiore a quello effettivo o *(ii)* elementi passivi fittizi o *(iii)* crediti e ritenute fittizi, quando, congiuntamente:

a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;
b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, *(i)* è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, *(ii)* è superiore a euro un milione cinquecentomila, ovvero *(iii)* 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.

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.

Ai fini dell'applicazione della norma 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.

- **Emissione di fatture o altri documenti per operazioni inesistenti (Art. 8, comma 1 e comma 2-bis, D.lgs. 10 marzo 2000, n. 74)**

La fattispecie di reato si realizza allorché un soggetto, 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.

Ai fini di quanto sopra indicato, 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.

- **Occultamento o distruzione di documenti contabili (Art. 10 D.lgs. 10 marzo 2000, n. 74)**

La fattispecie di reato si realizza allorché un soggetto, (i) al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero (ii) 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.

- **Sottrazione fraudolenta al pagamento di imposte (Art. 11 D.lgs. 10 marzo 2000, n. 74)**

La fattispecie di reato si realizza:

a) allorché un soggetto - *(i)* al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero *(ii)* 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.

b) allorché un soggetto - 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 (i) elementi attivi per un ammontare inferiore a quello effettivo o (ii) 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.

- **Dichiarazione infedele (Art. 4 D.lgs. 10 marzo 2000, n. 74)**

La fattispecie di reato si configura a carico di coloro che, al fine di evadere le imposte sui redditi o sul valore aggiunto, indicano, in una delle dichiarazioni 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 € 100.000,00;
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 € 2.000.000,00.
Ai fini dell'applicazione della predetta disposizione, 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.

In ogni caso, 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 della presente disosizione normativa, lettere a) e b). [In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, quando sono commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro]

- **Omessa dichiarazione (Art. 5 D.lgs. 10 marzo 2000, n. 74)**

La fattispecie di reato si realizza, allorquando, chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta , essendovi obbligato:

a) una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad € 50.000,00 ;

b) la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad € 50.000,00.

Ai fini delle disposizioni di cui sopra, 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. [In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, quando sono commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro]

- **Indebita compensazione (Art. 10 quater D.lgs. 10 marzo 2000, n. 74)**

La fattispecie di reato si configura a carico di coloro che: a) non versano le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, o crediti inesistenti per un importo annuo superiore a € 50.000,00.

legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai € 50.000,00. [In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, quando sono commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro].

- **Reati tributari non compresi nel novero dei Reati Presupposto**

Ai soli fini di chiarezza si precisa che non sono compresi nel novero dei Reati Presupposto tributari i seguenti ulteriori reati tributari (anch'essi previsti dal D.lgs. 10 marzo 2000, n. 74), dei quali pertanto risponde soltanto la persona fisica: Art. 6 Tentativo; Art. 9 Concorso di persone nei casi di emissione o utilizzazione di fatture o altri documenti per operazioni inesistenti; Art. 10-bis Omesso versamento di ritenute dovute o certificate; Art. 10-ter Omesso versamento di IVA.

Processi Sensibili

I Processi Sensibili che presentano il rischio di commissione dei Reati Presupposto di cui trattasi riguardano le seguenti attività: *(i)* emissione di documentazione afferente la contabilità; *(ii)* ricevimento di documentazione afferente la contabilità; *(iii)* predisposizione di dichiarazioni e comunicazioni concernenti la materia tributaria; *(iv)* presentazione di dichiarazioni e comunicazioni concernenti la materia tributaria; *(v)* pagamento di imposte.

Destinatari

Le regole di comportamento che seguono si applicano ai Destinatari che, a qualunque titolo, sono coinvolti nei Processi Sensibili sopra menzionati.

Regole di comportamento:

Rispetto della normativa e delle prescrizioni in materia

I Destinatari di cui sopra, ciascuno per quanto di rispettiva competenza, devono conoscere e rispettare e comunque, per quanto attiene agli organi sociali, far conoscere e far rispettare: *(i)* la normativa, e le istruzioni delle autorità preposte, in materia tributaria; *(ii)* le regole di cui al Modello; *(iii)* il Codice Etico; *(iv)* le procedure.

L'organizzazione aziendale deve garantire il rispetto delle normative in materia.

Organizzazione e poteri

In linea generale, il sistema di organizzazione per la gestione della materia in oggetto deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, e di segregazione delle funzioni e dei ruoli, in modo che nessun soggetto possa gestire da solo un intero processo, in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

Ai componenti degli organi sociali e ai dipendenti che per conto della Società intrattengono rapporti con la Agenzia delle Entrate e le autorità fiscali deve essere attribuito formale potere in tal senso. I soggetti muniti di poteri verso l'esterno devono agire nei limiti dei poteri ad essi conferiti. I soggetti privi di poteri verso l'esterno devono richiedere l'intervento dei soggetti muniti di idonei poteri.

Qualunque criticità o conflitto di interesse che dovessero sorgere nell'ambito del rapporto con le autorità fiscali devono essere comunicati, per iscritto, anche all'ODV.

Obblighi e divieti di carattere generale

a) I Destinatari non devono perseguire finalità di evasione di imposte sui redditi o sul valore aggiunto, o di altre imposte in generale, né nell'interesse o vantaggio della Società né nell'interesse o vantaggio di terzi.

b) I Destinatari, nelle dichiarazioni relative a dette imposte, e nella loro predisposizione, non devono introdurre elementi passivi fittizi avvalendosi di fatture o altri documenti per operazioni inesistenti. A tale riguardo:

   (i) devono controllare che le fatture e i documenti contabili si riferiscano a prestazioni effettivamente svolte da parte dell'emittente delle fatture/documenti ed effettivamente ricevute dalla Società;

   (ii) non devono registrare nelle scritture contabili obbligatorie, né detenere a fini di prova nei confronti dell'amministrazione finanziaria, fatture o altri documenti per operazioni inesistenti;

   (iii) devono verificare la regolare applicazione dell'imposta sul valore aggiunto.

c) I Destinatari devono astenersi *(i)* dal compiere operazioni simulate oggettivamente o soggettivamente nonché *(ii)* dall'avvalersi di documenti falsi o di altri mezzi fraudolenti idonei a ostacolare l'accertamento e a indurre in errore l'amministrazione finanziaria.

d) I Destinatari devono astenersi dall'indicare in dichiarazioni relative alle imposte sui redditi o sul valore aggiunto: *(i)* elementi attivi per un ammontare inferiore a quello effettivo o *(ii)* elementi passivi fittizi o *(iii)* crediti e ritenute fittizi.

e) I Destinatari devono astenersi dall'emettere o rilasciare fatture o altri documenti per operazioni inesistenti al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto.

f) I Destinatari devono astenersi dall'occultare o distruggere 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, con il fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi.

g) I Destinatari devono astenersi dall'alienare simulatamente o dal compiere altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva da parte dell'amministrazione finanziaria, con il fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte.

h) I Destinatari devono altresì astenersi dall'indicare nella documentazione presentata

   ai fini della procedura di transazione fiscale *(i)* elementi attivi per un ammontare inferiore a quello effettivo o *(ii)* elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila, con il fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori.

Approvazione da parte del responsabile apicale della gestione contabile e fiscale

Le dichiarazioni e comunicazioni in materia di imposte sui redditi o sul valore aggiunto non devono essere presentate senza la preventiva approvazione e benestare del Responsabile della funzione competente.

Tracciabilità

La Società deve seguire regole che garantiscano il rispetto della normativa in materia nonché la tracciabilità e trasparenza delle scelte operate, mantenendo a disposizione dell'ODV tutta la documentazione di supporto.

Ricorso a servizi di terzi

Nel caso in cui la predisposizione delle dichiarazioni e comunicazioni in materia di imposte sui redditi o sul valore aggiunto fosse affidata a terzi esterni alla Società, i terzi stessi dovranno essere vincolati contrattualmente a rispettare gli obblighi e i divieti di cui al par. 4.4. che precede.

In particolare in detti contratti deve essere contenuta apposita dichiarazione delle controparti:

a) di essere a conoscenza della normativa di cui al D.lgs. 231/2001 e delle sue implicazioni per la Società;

b) di impegnarsi a rispettare detta normativa e farla rispettare dai propri dipendenti e collaboratori;

c) di non essere mai stati condannati (o avere richiesto il patteggiamento) e di non essere al momento imputati o indagati in procedimenti penali relativi ai Reati Presupposto; nel caso di esistenza di condanna o di procedimento in corso, e sempre che l'accordo sia ritenuto indispensabile e da preferirsi a un contratto con altri soggetti, dovranno essere adottate particolari cautele;

d) di impegno a rispettare il Modello (ed in particolare le prescrizioni della presente Parte Speciale) e il Codice Etico della Società, ovvero, nel caso di enti, di avere adottato un proprio analogo Modello e un Codice Etico che regolamentano la prevenzione dei reati contemplati nel Modello e nel Codice Etico della Società;

e) di impegnarsi in ogni caso ad astenersi dal compiere attività che possano configurare alcuno dei Reati Presupposto o che comunque si pongano in contrasto con la normativa e/o con il Modello;

f) di adeguare il servizio a eventuali richieste della Società fondate sulla necessità di ottemperare alla prevenzione dei Reati Presupposto di cui trattasi.

Inoltre, nei contratti con i consulenti e con i prestatori di servizi deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte dei prestatori delle norme di cui al D.lgs. 231/2001 (quali ad es. clausole risolutive espresse, penali).

Procedure

Devono essere osservati, e si richiamano, i protocolli e la Procedura allegati al presente Modello nonché le altre procedure interne della società.

Controllo

Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi ai Processi Sensibili di cui trattasi devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente eventuali situazioni di irregolarità o anomalie.

I controlli dell'Organismo di Vigilanza

Si richiamano i contenuti *(i)* della Parte Generale relativi all'Organismo di Vigilanza e *(ii)* della Parte Speciale Sezione Undicesima.

PARTE SPECIALE - SEZIONE DECIMA

Ricettazione, riciclaggio, autoriciclaggio (art. 25-octies)

Le Fattispecie di Reato Presupposto riconducibili alle tipologie dei reati di ricettazione, riciclaggio ed autoriciclaggio

Il Decreto Legislativo 231/2007 ha modificato l'impianto dei reati presupposto previsti dal D. Lgs. 231/2001, introducendo l'articolo 25-octies in tema di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita. Le fattispecie sono state ulteriormente estese dalla Legge 186/2014, con l'introduzione del reato di autoriciclaggio tra i reati presupposto della responsabilità amministrativa dell'Ente.
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 alla progettazione di un efficace sistema di controllo interno atto a prevenirlo.

Autoriciclaggio (art. 648-ter 1 cod. pen.)

Tale ipotesi di reato si configura nel caso in cui chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa. In tale caso è prevista la reclusione da uno a quattro anni e la multa da Euro 2.500 a Euro 12.500. La pena è aumentata quando il fatto sia commesso nell'esercizio di un'attività bancaria, finanziaria o professionale.

Aree Sensibili

In particolare, con riferimento al reato di autoriciclaggio, è necessario considerare come aree a rischio, oltre a quelle individuate nella Matrice dei Rischi allegata al presente Modello, ed all'attività di gestione della tesoreria e della cassa contanti, tutte quelle aree in cui possono essere commessi i delitti non colposi (cosiddetti "reati fonte") i cui proventi possono poi essere impiegati, sostituiti, trasferiti in attività economiche, finanziarie, imprenditoriali o speculative.
Sulla base del risk assessment effettuato, si ritiene che la maggior parte dei reati fonte è già ricompresa nei reati di cui al D. Lgs. 231/01, pertanto, tali delitti e le relative aree a rischio sono trattate nelle diverse parti speciali del presente Modello a cui si rimanda.
In particolare, si è ritenuto di dover considerare come potenziali reati fonte i Reati Tributari di cui al D. Lgs. 74/2000 "Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della legge 25 giugno 1999, n. 205" ed a tal fine, è stata dunque identificata come attività sensibile anche quella riguardante la predisposizione delle dichiarazioni fiscali.
Nel caso in cui le funzioni aziendali 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.

Eventuali modifiche o integrazioni delle suddette attività sensibili sono rimesse alla competenza dell'Organo Amministrativo che potrà procedere con la successiva attività di ratifica secondo quanto indicato nella Parte Generale del Modello.

Regole di comportamento

In particolare, la presente Parte Speciale prevede l'esplicito divieto per i componenti del Consiglio di Amministrazione, e, nella misura necessaria alle funzioni dagli stessi svolte, per i Dipendenti e Consulenti di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato tra quelle sopra considerate (art. 24-*octies* del D.lgs. 231/2001);

- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato rientranti tra quelle sopra descritte, possano potenzialmente diventarlo;
- violare i principi e le procedure aziendali previste nella presente sezione.

Ai fini dell'attuazione delle regole elencate nei precedenti paragrafi, devono rispettarsi, oltre ai principi generali contenuti nel presente Modello, le misure preventive specifiche qui di seguito descritte in relazione alle singole attività sensibili:

Gestione della tesoreria e della cassa

Per quanto concerne la gestione della tesoreria e delle casse contanti, la Società adotta una specifica procedura (generale, intersettoriale o settoriale) che preveda:

a) il divieto di utilizzo del contante o altro strumento finanziario al portatore (fermo restando eventuali eccezioni dettate da esigenze operative/gestionali oggettivamente riscontrabili, sempre per importi limitati e comunque rientranti nei limiti di legge), per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie, nonché il divieto di utilizzo di conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia;

b) l'obbligo di:

- utilizzare operatori finanziari abilitati per la realizzazione di ciascuna delle operazioni di cui alla precedente lettera a);
- utilizzare esclusivamente, nell'ambito della gestione delle transazioni finanziarie, operatori che attestino di essere muniti di presidi manuali e informatici e/o telematici atti a prevenire fenomeni di riciclaggio;

c) la verifica dei destinatari dei pagamenti;

d) la verifica di corrispondenza tra la transazione finanziaria disposta e la relativa documentazione di supporto disponibile;

e) il divieto di effettuare pagamenti in paesi diversi da quelli in cui risiede la controparte o in cui ha esecuzione il contratto.

f) Con riferimento alle operazioni da effettuare tramite cassa preveda:

g) le modalità di utilizzo della piccola cassa (incluse le tipologie di spese e i limiti di utilizzo);

h) le riconciliazioni periodiche delle giacenze della piccola cassa con il registro delle movimentazioni di cassa.

Inoltre, con riferimento ai conti correnti bancari definisca:

I. le modalità operative di apertura, movimentazione e chiusura dei conti correnti presso banche e istituzioni finanziarie;

II. le riconciliazioni periodiche dei conti corrente.

Infine, nell'ambito dell'attività sensibile, qualsiasi esponente aziendale coinvolto è tenuto a:

- prestare particolare attenzione ai pagamenti provenienti da o disposti in favore di istituti di credito esteri, soprattutto qualora gli stessi abbiano sede in "paradisi fiscali", così come individuati da organismi nazionali e/o internazionali riconosciuti (es. Agenzie delle Entrate, OCSE), nonché ai pagamenti provenienti da e disposti in favore di persone fisiche o giuridiche che abbiano residenza o sede in "paradisi fiscali";
- non eseguire disposizioni di pagamento in favore di soggetti che non siano correttamente identificabili, su conti correnti non indicati nel contratto, nell'ordine ovvero in altra documentazione condivisa con la controparte, su conti anonimi o cifrati;
- assicurare la correttezza e tracciabilità dei pagamenti effettuati, assicurando che ogni pagamento trovi adeguata giustificazione contrattuale e costituisca il corrispettivo per una prestazione realmente ricevuta.

Predisposizione delle dichiarazioni fiscali

Per quanto concerne la predisposizione delle dichiarazioni fiscali, la Società ha previsto la seguente regolamentazione:

a) un'adeguata modalità di archiviazione e conservazione, laddove possibile in via digitale, dei modelli dichiarativi e di versamento delle imposte sottoscritte dai soggetti autorizzati ed inviati all'Amministrazione Finanziaria e di ogni altra documentazione contabile di cui sia necessaria la conservazione ai fini fiscali;
b) una verifica della correttezza dei dati contabili rilevanti ai fini fiscali riportati nelle dichiarazioni annuali e periodiche funzionali all'assolvimento delle imposte, garantendo altresì la corretta liquidazione delle stesse;
c) l'esecuzione di controlli volti a verificare ex post il corretto invio telematico delle dichiarazioni fiscali, e che i dati riportati nella ricevuta di trasmissione corrispondano a quanto indicato nelle relative dichiarazioni trasmesse;
d) predisporre e monitorare, con cadenza periodica, le scadenze sugli adempimenti fiscali nel rispetto delle scadenze previste dalla normativa.

Inoltre, la Società assicura che l'individuazione di eventuali studi legali/tributari e/o professionisti esterni che supportano la Società nelle attività di gestione degli aspetti fiscali e del contenzioso fiscale avvenga secondo requisiti di professionalità, onorabilità e competenza e, in riferimento a essi, sia motivata la scelta. Il rapporto con il consulente esterno è formalizzato in un contratto che prevede apposita clausola con cui la controparte dichiara di essere a conoscenza del Codice di Condotta, e del Modello 231 e del Piano di prevenzione della corruzione adottati da Sardegna IT S.r.l. c.s.u. e delle loro implicazioni per la controparte, di accettarli e di impegnarsi a rispettarli, nonché apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Modello e/o al Codice di Condotta e/o al Piano di Prevenzione della corruzione di Sardegna IT S.r.l. c.s.u.

Procedure

Devono essere osservati, e si richiamano, i protocolli e la Procedura allegati al presente Modello nonché le altre procedure interne della società.

I controlli dell'Organismo di Vigilanza

Si richiamano i contenuti *(i)* della Parte Generale relativi all'Organismo di Vigilanza e *(ii)* della Parte Speciale Sezione Undicesima.

PARTE SPECIALE - SEZIONE UNDICESIMA

I controlli dell'Organismo di Vigilanza

Segnalazioni all'Organismo di Vigilanza

La Società fornirà all'ODV, oltre ai flussi di comunicazione previsti nella Parte Generale, le informazioni e la documentazione che fosse dallo stesso richiesta.
La Società segnalerà all'Organismo di Vigilanza le criticità che dovesse rilevare nell'ambito dei controlli di primo e secondo livello.
All'ODV viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Attività dell'Organismo di Vigilanza

L' ODV effettua in piena autonomia specifici controlli e, periodicamente, controlli a campione sulle attività connesse ai Processi Sensibili e sul rispetto dei Protocolli di cui alla Parte Speciale, diretti a verificare la corretta implementazione delle stesse in relazione alle prescrizioni di cui al Modello.
L'ODV segnalerà alla direzione della Società le anomalie o criticità che dovesse rilevare.