



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del Decreto Legislativo dell'8 giugno 2001 n. 231

PARTE SPECIALE

COMITATO REGIONALE CAMPANIA

Testo approvato dal Consiglio Direttivo del Comitato Regionale in data XX.XX.2014



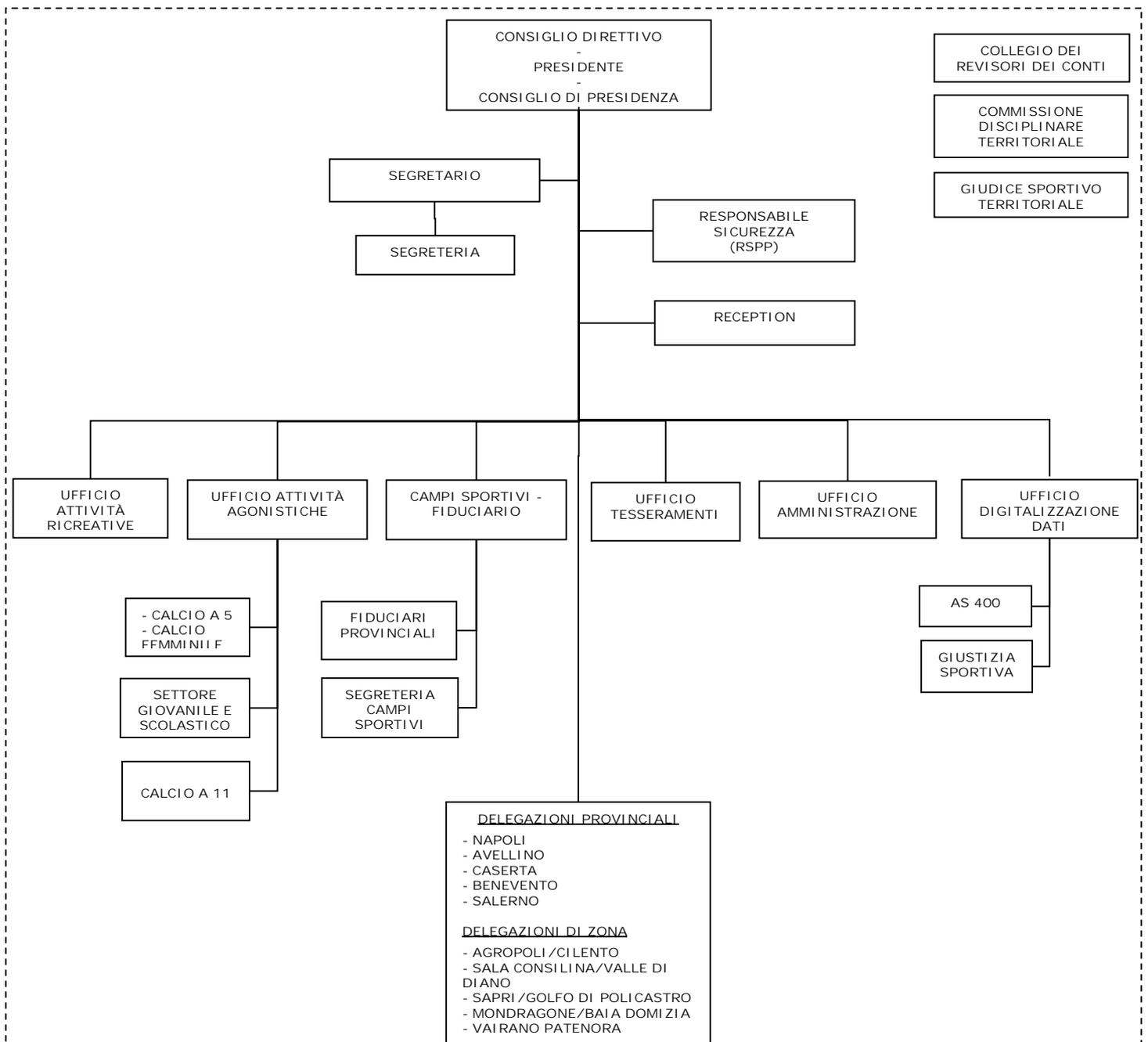
INDICE

ORGANIGRAMMA	3
A. REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE	4
B. REATI SOCIETARI	10
C. I REATI DI RICICLAGGIO	17
D. I REATI COMMESSI CON LA VIOLAZIONE DELLE NORME ANTI INFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO	24
E. DELITTI INFORMATICI	29
F. REATI CONTRO LA PERSONALITA' INDIVIDUALE	38



ORGANIGRAMMA

L'Organigramma del Comitato Regionale è parte integrante del Modello e viene aggiornato in occasione di ogni sua variazione significativa.





A. REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

La presente “Parte Speciale” del Modello si riferisce ai reati realizzabili nell’ambito dei rapporti tra il Comitato Regionale Campania (di seguito anche il “Comitato Regionale”) e la Pubblica Amministrazione. Si descrivono brevemente qui di seguito le fattispecie contemplate dal Decreto, che potrebbero trovare eventualmente manifestazione all’interno del Comitato Regionale.

A.1 Ipotesi di reato

Corruzione per un atto d’ufficio (artt. 318, 320 e 321 c.p.)

Tale ipotesi di reato si configura nel caso in cui venga data o promessa a un pubblico ufficiale o a un incaricato di pubblico servizio, per sé o per altri, in denaro o altra utilità, una retribuzione che non gli è dovuta per compiere ovvero per avere compiuto un atto del suo ufficio. Il reato si configura sia nei confronti del corrotto sia del corruttore.

Corruzione per un atto contrario ai doveri d’ufficio (artt. 319, 320 e 321 c.p.)

Tale ipotesi di reato si configura nel caso in cui venga data o promessa a un pubblico ufficiale o un incaricato di pubblico servizio, per sé o per altri, denaro o altra utilità per omettere o ritardare, per aver omesso o ritardato, un atto del suo ufficio ovvero per compiere o per avere compiuto un atto contrario ai doveri d’ufficio. Il reato si configura sia nei confronti del corrotto sia del corruttore.

Circostanze aggravanti (art. 319-bis c. p.)

Tale disposizione prevede che la pena è aumentata se il fatto abbia per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l’amministrazione alla quale il pubblico ufficiale appartiene.

Corruzione in atti giudiziari (artt. 319 ter e 321 c.p.)

Tale ipotesi di reato si configura nel caso in cui i fatti di cui agli artt. 318 e 319 c.p. (corruzione per un atto di ufficio e/o corruzione per un atto contrario ai doveri d’ufficio)



siano commessi al fine di favorire o danneggiare una parte in un procedimento civile, penale o amministrativo.

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

Tale ipotesi di Reato si configura nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induca taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra.

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

Tale ipotesi di reato si configura nel caso in cui venga offerto denaro o altra utilità a un pubblico ufficiale o ad un incaricato di pubblico servizio per una finalità corruttiva qualora l'offerta o la promessa non sia accettata.

Malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui un soggetto estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità Europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina a predette attività.

Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316-ter c.p.)

Tale ipotesi di reato si configura nei casi in cui, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere ovvero mediante l'omissione di informazioni dovute, si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominati, concessi o erogati dallo Stato, da altri enti pubblici o dalla Comunità europea. In questo caso, contrariamente a quanto visto in merito al punto precedente, a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti. Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie di cui all'art. 640-bis c.p. (truffa aggravata per il conseguimento di erogazioni pubbliche), nel senso che si configura solo nei casi in cui la condotta non integri gli estremi del reato di cui a quest'ultima disposizione.



Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640 c.p.)

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

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

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche. 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.

Concussione (art. 317 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua qualità o dei suoi poteri, costringa o induca taluno a dare o a promettere indebitamente a sé o ad altri denaro o altre utilità. Ferma restando la natura privatistica della L.N.D., nella convinzione che l'adozione del Modello, sebbene facoltativa e non obbligatoria ai sensi del Decreto, possa costituire un valido strumento di sensibilizzazione di tutti coloro che operano in nome e per conto della L.N.D. a tenere condotte conformi alla normativa vigente, nonché in un'ottica di perseguimento della best practice nello svolgimento dell'attività associativa.

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)

Tale ipotesi di reato si configura nel caso in cui, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi. In concreto, può integrarsi il reato in esame qualora, una volta ottenuto un finanziamento, sia violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente. Il reato è punibile a querela di parte.



A.2. Individuazione delle attività sensibili

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione.

Tenuto conto dell'operatività del Comitato Regionale Campania, costituiscono attività sensibili ai sensi del Decreto le seguenti attività:

- ✓ Intrattenere rapporti con la Pubblica Amministrazione per l'organizzazione delle manifestazioni di sua competenza, la gestione delle strutture sportive, la normativa in ambito sportivo ed eventuali contributi/convenzioni;
- ✓ Occuparsi della gestione delle controversie giudiziali e stragiudiziali (ad es. selezione degli avvocati, rapporti con la magistratura, etc.)
- ✓ Distribuire alle Società i contributi federali e quelli concessi dalla L.N.D. e dagli Organi collegati;
- ✓ Aderire al progetto di creazione di un "centro sportivo federale" in tutte le regioni d'Italia promosso dalla L.N.D.;
- ✓ Omologare i campi da calcio (ivi inclusi quelli di calcio femminile e calcio a 5) di competenza in conformità alle norme federali vigenti.

A.3. Individuazione delle funzioni coinvolte

Tenuto conto dell'operatività del Comitato Regionale Campania, gli uffici ed i soggetti apicali ritenuti più specificamente a rischio sono:

- ✓ Presidente;
- ✓ Consiglio Direttivo;
- ✓ Segretario;
- ✓ Responsabile Amministrativo;
- ✓ Delegati Provinciali;
- ✓ Fiduciario Campi Sportivi.



A.4. Presidi organizzativi

I presidi organizzativi/controlli *specifici* posti in essere dal Comitato Regionale Campania, in relazione alle sopra indicate attività sensibili, che possono essere considerati a prevenzione a fronte dei reati contro la Pubblica Amministrazione, prevedono che:

- ✓ Sia prevista una specifica indicazione da parte del Consiglio Direttivo del Comitato in merito a chi è autorizzato a gestire i rapporti con la Pubblica Amministrazione;
- ✓ Il processo di autorizzazione al pagamento delle fatture d'acquisto sia sottoposto preventivamente ad un duplice controllo: da parte della risorsa che ha predisposto il bonifico e da parte di coloro che autorizzano il pagamento (firma congiunta del Presidente e del Segretario o, in assenza del Presidente, del Vice Presidente e del Segretario);
- ✓ Sia vietato assegnare incarichi di fornitura a persone o società vicine o gradite a soggetti pubblici in assenza dei necessari requisiti di qualità, sicurezza e convenienza dell'operazione di acquisto;
- ✓ Ai sensi del Titolo VI del Regolamento Amministrativo Contabile della L.N.D., i contributi ricevuti siano utilizzati e/o distribuiti alle Società secondo criteri fissati dall'Ente erogante. Solo il Consiglio Direttivo previa autorizzazione dell'Ente erogante può deliberare un diverso criterio di ripartizione dei contributi dei quali devono comunque beneficiare tutte le Società appartenenti al Comitato;
- ✓ La stipula di accordi/contratti/convenzioni con controparte la P.A. sia preventivamente autorizzata e deliberata dal Consiglio Direttivo che ne effettua una valutazione di merito e successivamente rendicontata allo stesso affinché ne verifichi la corretta esecuzione;
- ✓ L'omologazione dei campi sportivi sia effettuata secondo le linee guida emanate dalla L.N.D. in materia e svolta da professionisti qualificati i quali redigono un apposito verbale a firma del Fiduciario Campi Sportivi del Comitato.



I presidi organizzativi *generici* che devono essere posti in essere dalla Comitato Regionale (Codici, Misure organizzative, Sistemi informatici, Procedure), a fronte dei reati contro la Pubblica Amministrazione, sono i seguenti:

- ✓ Esplicita previsione tra i principi del Codice Etico del divieto di pratiche corruttive;
- ✓ E' fatto divieto, in particolare, agli organi sociali, ai dirigenti, ai dipendenti e collaboratori del Comitato Regionale:
 - effettuare elargizioni in denaro a pubblici funzionari italiani;
 - promettere o versare somme o beni in natura a qualsiasi soggetto (sia esso un dirigente, funzionario o dipendente della Pubblica Amministrazione o un soggetto privato) per promuovere o favorire gli interessi del Comitato anche a seguito di illecite pressioni.
 - ricorrere a forme diverse di aiuti o contribuzioni che, sotto veste di sponsorizzazioni, incarichi, consulenze o pubblicità abbiano invece le stesse finalità sopra vietate;
- ✓ Diffusione del Codice Etico verso tutti i Dipendenti;
- ✓ Controllo dei flussi finanziari in uscita dal Comitato;
- ✓ Controllo della documentazione e, in particolare, delle fatture passive (la pratica più diffusa per procurarsi la provvista per corrompere è l'utilizzazione di fatture per operazioni inesistenti);
- ✓ Programma di informazione/formazione periodica del Dipendente.
- ✓ Coerenza delle procure verso l'esterno con il sistema delle deleghe;
- ✓ Esclusione esplicita, nel sistema delle procure, della "richiesta di denaro o altra utilità a terzi".

In allegato sono riportati criteri per la classificazione dei soggetti, se pubblici o privati.



B. REATI SOCIETARI

La presente “Parte Speciale” del Modello si riferisce ai reati societari. Si descrivono brevemente qui di seguito le fattispecie contemplate dal Decreto, che potrebbero trovare eventualmente manifestazione all’interno del Comitato Regionale.

B.1. Ipotesi di reato

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

Tale ipotesi di reato si configura nei casi in cui, con l’intenzione di ingannare gli associati o il pubblico e al fine di conseguire per sé o per altri ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette agli associati o al pubblico, si espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazioni, ovvero si omettono informazioni la cui comunicazione è imposta dalla legge, sulla situazione economica, patrimoniale o finanziaria della L.N.D., in modo idoneo a indurre in errore i destinatari sulla predetta situazione.

False comunicazioni sociali in danno dei soci o dei creditori (art. 2622 c.c.)

Tale ipotesi di reato si configura nei casi in cui, con l’intenzione di ingannare gli associati o il pubblico e al fine di conseguire per sé o per gli altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette agli associati o al pubblico, esponendo fatti materiali non rispondenti al vero ancorché oggetto di valutazioni, ovvero omettendo informazioni la cui comunicazione è imposta dalla legge, sulla situazione economica, patrimoniale o finanziaria della L.N.D., in modo idoneo a indurre in errore i destinatari sulla predetta situazione, si cagiona un danno patrimoniale agli associati o ai creditori.

Impedito controllo (art. 2625, comma 2 c.c.)

Tale ipotesi di reato si configura nel caso in cui gli amministratori, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle



attività di controllo o di revisione, legalmente attribuite agli associati, ad altri Organi Sociali, e cagionano un danno per gli stessi associati.

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

Tale ipotesi di reato si configura nel caso in cui gli amministratori, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altre società/associazioni o scissioni, cagionando un danno ai creditori.

Corruzione tra privati (art. 2635 c.c.)

Tale ipotesi di Reato si configura nel caso in cui gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiano od omettano atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società.

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

Tale ipotesi di reato si configura nel caso in cui, con atti simulati o fraudolenti, si determina la maggioranza in assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto.

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

Tale ipotesi di reato si configura nel caso in cui gli amministratori, i direttori generali, i sindaci ed i liquidatori di società od enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti in tutto o in parte fatti che avrebbero dovuto comunicare concernenti la situazione medesima.

La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dal Comitato Regionale Campania per conto di terzi. Tale ipotesi di reato si



configura altresì nel caso in cui gli amministratori, i direttori generali, i sindaci ed i liquidatori di società od enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.

B.2. Individuazione delle attività sensibili

Costituiscono situazioni di particolare attenzione in riferimento alle suddette fattispecie di reato le seguenti attività:

- ✓ Predisporre e approvare il piano economico per obiettivi (P.E.P.O.) nonché il bilancio di esercizio annuale del Comitato Regionale;
- ✓ Eseguire tutti gli atti di natura amministrativo-contabile diretti al conseguimento dei fini istituzionali;
- ✓ Gestisce la partecipazione, come socio unico, di una società immobiliare a responsabilità limitata proprietaria della sede centrale del Comitato;
- ✓ Omologare i campi di calcio (ivi inclusi quelli di calcio femminile e calcio a 5) di sua competenza in conformità alle norme federali vigenti;
- ✓ Utilizzare collaboratori/volontari per supportare le attività dei propri dipendenti sia presso la sede sia presso le delegazioni provinciali del Comitato Regionale;
- ✓ Intrattenere rapporti con la L.N.D. per la gestione del Personale, la realizzazione e gestione dei sistemi informativi e la gestione dell'attività commerciale (per il tramite della LND Servizi SRL);
- ✓ Curare la stesura, la pubblicazione e la raccolta dei Comunicati Ufficiali e delle Circolari del Comitato Regionale;
- ✓ Aprire e gestire i conti correnti bancari per l'espletamento dei servizi di riscossione e pagamento;
- ✓ Curare la gestione dei rapporti con il Collegio dei Revisori della L.N.D.



B.3. Individuazione delle funzioni coinvolte

Tenuto conto dell'operatività del Comitato Regionale Campania, gli uffici ed i soggetti apicali ritenuti più specificamente a rischio sono:

- ✓ Presidente;
- ✓ Consiglio Direttivo;
- ✓ Consiglio di Presidenza;
- ✓ Segretario;
- ✓ Responsabile Amministrativo;
- ✓ Ufficio Amministrazione.

B.4. Presidi organizzativi

I presidi organizzativi/controlli *specifici* posti in essere dal Comitato Regionale Campania, in relazione alle sopra indicate attività sensibili, che possono essere considerati a prevenzione dei reati di false comunicazioni sociali e illecite operazioni sulle azioni o quote sociali o della società controllante, prevedono che:

- ✓ Tutto il processo di formazione del bilancio e di altri documenti similari sia sottoposto ad attente attività di controllo da parte di soggetti diversi. In particolare, sia previsto un duplice controllo da parte dell'Ufficio Amministrazione e del Responsabile Amministrativo ed uno successivo da parte del Collegio dei Revisori dei Conti;
- ✓ Il bilancio sia portato all'attenzione del Consiglio di Presidenza e approvato dal Consiglio Direttivo del Comitato;
- ✓ Il Collegio dei Revisori dei Conti nella propria relazione in allegato al bilancio esprima le proprie valutazioni in merito al rispetto dei corretti principi di amministrazione da parte del Comitato in conformità alla legge, allo statuto, al R.A.C. e anche in relazione alle procedure di controllo interno adottate.



- ✓ I comunicati e le circolari ufficiali di maggior rilievo della L.N.D., prima della loro pubblicazione, siano visionati e approvati dal Presidente.

I presidi organizzativi/controlli *specifici* posti in essere dal Comitato, in relazione alle sopra indicate attività sensibili, che possono essere considerati a prevenzione del reato di corruzione tra privati, prevedono che:

- ✓ Tutti i pagamenti effettuati ai fornitori siano preventivamente controllati e autorizzati come previsto dal Regolamento Amministrativo Contabile (di seguito "R.A.C.") della L.N.D.;
- ✓ Il processo di autorizzazione al pagamento delle fatture d'acquisto sia sottoposto preventivamente ad un duplice controllo: da parte della risorsa che ha predisposto il bonifico e da parte di coloro che autorizzano il pagamento (firma congiunta del Presidente e del Segretario, in assenza del Presidente, del Vice Presidente e del Segretario);
- ✓ Le attività di selezione e l'iter autorizzativo dei fornitori di servizi e beni necessari per l'organizzazione degli eventi siano svolte secondo le regole dettate dal R.A.C.

I presidi organizzativi/controlli *specifici* posti in essere dal Comitato, in relazione alle sopra indicate attività sensibili, che possono essere considerati a prevenzione dei reati di impedito controllo, prevedono che:

- ✓ Tutti i documenti necessari per le verifiche del Collegio dei Revisori siano sempre disponibili presso l'Ufficio Amministrazione;
- ✓ Tutti gli obblighi societari, civilistici e contabili siano verificati dal Collegio dei Revisori, oltre che dall'Ufficio Amministrazione e dal Responsabile Amministrativo;
- ✓ La tenuta della contabilità generale sia affidata all'Ufficio Amministrazione, sotto la responsabilità del Responsabile Amministrativo. Inoltre, tutti i pagamenti effettuati ai fornitori siano preventivamente controllati e autorizzati come previsto R.A.C. della L.N.D.



I presidi organizzativi/controlli *specifici* posti in essere dal Comitato, in relazione alle sopra indicate attività sensibili, che possono essere considerati a prevenzione dei reati di illecita influenza sull'assemblea, prevedono che:

- ✓ Ogni intervento del Presidente e del Segretario nel Consiglio Direttivo/Presidenza sia verbalizzato ed archiviato insieme alla documentazione di supporto, ove presente.

I presidi organizzativi/controlli *specifici* posti in essere dal Comitato, in relazione alle sopra indicate attività sensibili, che possono essere considerati a prevenzione dei reati di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, prevedono che:

- ✓ Vi sia una responsabilità primaria da parte del Presidente, o persona da lui delegata, nell'espletamento di tutti gli adempimenti richiesti dagli organi di vigilanza.

I presidi organizzativi *generici* che possono essere posti in essere dal Comitato (Codici, Misure organizzative, Sistemi informatici, Procedure), a fronte dei reati societari, sono i seguenti:

- ✓ Inserimento nelle norme di comportamento (o Codice Etico) adottate dalla L.N.D. di specifiche previsioni riguardanti il corretto comportamento di tutti i Dipendenti e Collaboratori coinvolti nelle attività di formazione del bilancio o di altri documenti simili. Ad esempio: massima collaborazione; completezza e chiarezza delle informazioni fornite; accuratezza dei dati e delle elaborazioni; segnalazione di conflitti di interesse; etc.
- ✓ Attività di formazione di base verso determinate risorse coinvolte nel processo di formazione del bilancio, affinché conoscano almeno le principali nozioni sul bilancio (norme di legge, sanzioni, principi contabili, ecc.).
- ✓ Istituzione di una procedura chiara e tempificata rivolta alle stesse risorse di cui sopra, 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" (vedi R.A.C.).



- ✓ Previsione dell'obbligo - per il responsabile di funzione che fornisce dati ed informazioni relative al bilancio o ad altre comunicazioni sociali - di inserire il proprio visto di veridicità e completezza sulle informazioni trasmesse.
- ✓ Tempestiva messa a disposizione di tutti i componenti del Consiglio Direttivo della bozza del bilancio, prima della riunione del Consiglio per l'approvazione dello stesso; il tutto con una documentata certificazione dell'avvenuta consegna della bozza in questione.



C. I REATI DI RICICLAGGIO

La presente “Parte Speciale” del Modello si riferisce ai reati di riciclaggio. Si descrivono brevemente qui di seguito le fattispecie contemplate dal Decreto, che potrebbero trovare eventualmente manifestazione all’interno del Comitato Regionale Campania.

C.1. Ipotesi di reato

I reati di riciclaggio

Il Comitato Regionale, nello svolgimento della propria attività, in particolare attraverso operazioni sul contante e/o su strumenti finanziari, potrebbe commettere o favorire i seguenti reati:

Ricettazione (art. 648 c.p.)

Lo scopo dell’incriminazione della ricettazione è quello di impedire il perpetrarsi della lesione di interessi patrimoniali iniziata con la consumazione del reato principale. Ulteriore obiettivo della incriminazione consiste nell’evitare la commissione dei reati principali, come conseguenza dei limiti posti alla circolazione dei beni provenienti dai reati medesimi. L’art. 648 c.p. incrimina chi “fuori dei casi di concorso nel reato, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare”. Per acquisto dovrebbe intendersi l’effetto di un’attività negoziale, a titolo gratuito od oneroso, mediante la quale l’agente consegue il possesso del bene. Il termine ricevere starebbe ad indicare ogni forma di conseguimento del possesso del bene proveniente dal delitto, anche se solo temporaneamente o per mera compiacenza. Per occultamento dovrebbe intendersi il nascondimento del bene, dopo averlo ricevuto, proveniente dal delitto. La ricettazione può realizzarsi anche mediante l’intromissione nell’acquisto, nella ricezione o nell’occultamento della cosa. Tale condotta si esteriorizza in ogni attività di mediazione, da non intendersi in senso civilistico (come precisato dalla giurisprudenza), tra l’autore del reato principale e il terzo acquirente. Il reato di ricettazione può essere realizzato in molte aree e a più livelli organizzativi. Tuttavia, devono essere maggiormente monitorate



alcune funzioni/aree/processi esposti maggiormente a rischio, come il settore acquisiti o quello commerciale. L'ultimo comma dell'art. 648 c.p. estende la punibilità "anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto".

Riciclaggio (art. 648-bis c.p.)

Lo scopo dell'incriminazione del reato di riciclaggio è quello di impedire che gli autori dei reati possano far fruttare i capitali illegalmente acquisiti, rimettendoli in circolazione come capitali ormai "depurati" e perciò investibili anche in attività economiche produttive lecite. In tal modo, la norma incriminatrice persegue anche un ulteriore obiettivo finale, vale a dire scoraggiare la stessa commissione dei reati principali, mediante le barriere frapposte alla possibilità di sfruttarne i proventi. L'art. 648-bis c.p. incrimina chiunque "fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa". Per sostituzione si intende la condotta consistente nel rimpiazzare il denaro, i beni o le altre utilità di provenienza illecita con valori diversi. Il trasferimento consiste nella condotta tendente a ripulire il denaro, i beni o le altre utilità mediante il compimento di atti negoziali. Le operazioni idonee ad ostacolare l'identificazione dell'illecita provenienza potrebbero essere considerate quelle in grado di intralciare l'accertamento da parte della autorità giudiziaria della provenienza delittuosa dei valori provenienti dal reato. Le attività esposte a rischio anche per questa tipologia di reato sono diverse, anche se maggiore attenzione dovrà essere rivolta ai settori commerciale e amministrativo-finanziario. Il terzo comma dell'articolo in esame richiama l'ultimo co. dell'art. 648 c.p. già esaminato.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)

Il delitto in esame risponde ad una duplice finalità: mentre in un primo momento occorre impedire che il cd. "denaro sporco", frutto dell'illecita accumulazione, venga trasformato in denaro pulito, in un seconda fase è necessario fare in modo che il capitale, pur così emendato dal vizio di origine, non possa trovare un legittimo impiego. La clausola di riserva contenuta nel co. 1 della disposizione in commento prevede la punibilità



solamente di chi non sia già compartecipe del reato principale ovvero non sia imputabile a titolo di ricettazione o riciclaggio. Da ciò deriva che per la realizzazione della fattispecie *de qua* occorre la presenza, quale elemento qualificante rispetto alle altre figure criminose citate, di una condotta di impiego dei capitali di provenienza illecita in attività economiche o finanziarie. La condotta incriminata consiste nell'impiego dei capitali di provenienza illecita in attività economiche o finanziarie. Impiegare è sinonimo di usare comunque, ossia un utilizzo per qualsiasi scopo. Tuttavia, considerato che il fine ultimo perseguito dal legislatore consiste nell'impedire il turbamento del sistema economico e dell'equilibrio concorrenziale attraverso l'utilizzo di capitali illeciti reperibili a costi inferiori rispetto a quelli leciti, si ritiene che per impiegare debba intendersi, in realtà, investire. Dovrebbe, quindi, ritenersi rilevante un utilizzo a fini di profitto.

Tali reati, infine, che possono avere valenza nazionale e/o transnazionale, si configurano ogniqualvolta si possa rientrare, anche in via indiretta, nell'ambito del favoreggiamento delle organizzazioni criminali, attuato tramite la facilitazione del riciclaggio di fondi di provenienza illecita o il concorso nel finanziamento alle organizzazioni stesse, a causa dell'omissione degli opportuni controlli sulla persona disponente e beneficiaria dell'operazione nonché sulla natura stessa dell'operazione.

C.2. Individuazione delle attività sensibili

Tenuto conto dell'operatività del Comitato Regionale Campania, costituiscono attività sensibili ai sensi del Decreto le seguenti attività:

- ✓ Gestire gli incassi dalle Società per l'iscrizione ai Campionati e ai Tornei di sua competenza e occuparsi del recupero degli eventuali crediti;
- ✓ Curare il tesseramento dei giocatori e della gestione dei relativi incassi dalle Società di appartenenza;
- ✓ Occuparsi della gestione economica delle Delegazioni Provinciali;
- ✓ Istituire il servizio di cassa interno e gestire la relativa Cassa Contanti del Comitato;



- ✓ Occuparsi dell'accensione/gestione/chiusura dei conti delle Società e dei relativi addebiti e accrediti (spese sostenute dal Comitato, sanzioni pecuniarie Organi di Giustizia Sportiva, etc.);
- ✓ Organizzare e gestire, su autorizzazione della L.N.D., attività di formazione dei Dirigenti delle Società associate che a vario titolo prestano la loro opera all'interno della struttura;
- ✓ Assumere impegni di spesa nell'ambito delle previsioni del P.E.P.O. e nelle modalità e limiti previsti dal R.A.C.;
- ✓ Aprire e gestire i conti correnti bancari per l'espletamento dei servizi di riscossione e pagamento;
- ✓ Occuparsi della liquidazione delle spese arbitrali relative ai Tornei e/o Gare amichevoli preventivamente autorizzate.

C.3. Individuazione delle funzioni coinvolte

Tenuto conto dell'operatività del Comitato Regionale, gli uffici ed i soggetti apicali ritenuti più specificamente a rischio sono:

- ✓ Presidente;
- ✓ Segretario;
- ✓ Responsabile Amministrativo;
- ✓ Ufficio Amministrazione;
- ✓ Cassiere;
- ✓ Ufficio Tesseramenti;
- ✓ Delegazioni Provinciali.



C.4. Presidi organizzativi

I presidi organizzativi/controlli *specifici* posti in essere dal Comitato Regionale, in relazione alle sopra indicate attività sensibili, che possono essere considerati a prevenzione dei reati di riciclaggio, prevedono che:

- ✓ Le attività di selezione e l'iter autorizzativo dei fornitori di servizi e beni siano svolte secondo le regole dettate dal R.A.C.;
- ✓ Gli ordini di bonifico siano predisposti dall'Ufficio Amministrazione mentre per l'autorizzazione sia necessaria la firma congiunta del Presidente e del Segretario o, in assenza del Presidente, del Vice Presidente e del Segretario. Sia rispettato quindi il principio della separazione funzionale e della contrapposizione operativa tra chi predispone i pagamenti bancari e chi li autorizza;
- ✓ Sia verificata da parte dell'Ufficio Amministrazione la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- ✓ La stipula dei contratti di vendita o locazione di immobili sia preventivamente deliberata dal Consiglio Direttivo dopo un'attenta attività di controllo che miri a verificare che l'operazione sia effettuata nel rispetto delle disposizioni in tema di antiriciclaggio;
- ✓ Tutti i passaggi di denaro ordinari tra il Comitato e la società controllata siano regolamentati da appositi contratti di service con la descrizione degli importi e delle modalità di pagamento;
- ✓ Per il tesseramento dei giocatori e l'iscrizione ai Campionati, Tornei e Gare amichevoli organizzate dal Comitato, siano ritenuti ammissibili solo i pagamenti, se di importo superiore ai 516,46 Euro, effettuati dalle società sportive tramite conti correnti bancari o postali a loro intestati ovvero secondo altre modalità idonee a consentire all'amministrazione finanziaria lo svolgimento di efficaci controlli;
- ✓ Nel rispetto della soglia di 516,46 €, non siano accettati pagamenti in contanti frazionati oltre la somma totale di 15.000 €



- ✓ Non siano effettuati pagamenti in contanti superiori o uguali alla soglia di € 1.000;
- ✓ Ai sensi dell'art. 54 del R.A.C. la Cassa contanti sia alimentata con prelievi diretti dal c/c bancario ordinario del Comitato e la sua giacenza non può superi i 2.000 € La Cassa sia, inoltre, utilizzata per spese non superiori ai 200 € ed esse siano sempre giustificate con idonea documentazione. Gli eventuali titoli di credito ricevuti, infine, siano quotidianamente versati sul c/c del Comitato;
- ✓ Le rimesse di contante da parte delle Delegazioni Provinciali verso la sede centrale del Comitato Regionale siano effettuate esclusivamente attraverso sistemi di pagamento tracciabili.

I presidi organizzativi *generici* che devono essere posti in essere dal Comitato Regionale Campania (Codici, Misure organizzative, Sistemi informatici, Procedure), a fronte dei reati di riciclaggio sono i seguenti:

- ✓ Verifica dell'attendibilità commerciale e professionale dei fornitori e partner commerciali, sulla base di alcuni indici rilevanti (es. dati pregiudizievoli pubblici, protesti, procedure concorsuali o acquisizione di informazioni commerciali sulla azienda, sui soci e sugli amministratori tramite società specializzate; entità del prezzo sproporzionata rispetto ai valori medi di mercato; coinvolgimento di "persone politicamente esposte", come definite all'art. 1 dell'Allegato tecnico del d.lgs. 21 novembre 2007, n. 231, di attuazione della direttiva 2005/60/CE);
- ✓ Controlli formali e sostanziali dei flussi finanziari, con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni infragruppo;
- ✓ Determinazione dei requisiti minimi in possesso dei soggetti offerenti e fissazione dei criteri di valutazione delle offerte nei contratti standard (vedi R.A.C.);
- ✓ Specifica previsione di regole disciplinari in materia di prevenzione dei fenomeni di riciclaggio;



- ✓ Adozione di adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.



D. I REATI COMMESSI CON LA VIOLAZIONE DELLE NORME ANTI INFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

La presente "Parte Speciale" del Modello Organizzativo si riferisce ai reati di omicidio colposo e lesioni gravissime commessi con violazione delle norme anti-infortunistiche, sulla tutela dell'igiene e della salute sul lavoro. Si descrivono brevemente qui di seguito le fattispecie contemplate dal Decreto, che potrebbero trovare eventualmente manifestazione all'interno del Comitato Regionale.

D.1. Ipotesi di reato

Omicidio colposo (art. 589 c.p.) e lesioni personali gravi o gravissime (art. 590, c.3 c.p.)

Con Legge 3 agosto 2007 n. 123, recante "Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa in materia" è stato introdotto nel Decreto l'art. 25 septies, come sostituito nella sua attuale stesura dall'art. 300 d.lgs. 9 aprile 2008 n. 81, che ha esteso il novero dei reati cd. presupposto all'omicidio colposo e alle lesioni colpose gravi o gravissime commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro. Le condotte punite dalle due fattispecie consistono nel cagionare per colpa, rispettivamente, la morte oppure una lesione dalla quale deriva una malattia, nel corpo o nella mente, grave o gravissima. Per lesioni gravi s'intendono quelle consistenti in una malattia che metta in pericolo la vita o provochi un'incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai quaranta giorni, oppure in un indebolimento permanente di un senso o di un organo. Per lesioni gravissime s'intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso.

A completamento del corpo normativo delineato dalle specifiche misure di prevenzione prescritte dalle leggi in materia si colloca la più generale previsione di cui all'art. 2087 del c.c., in forza della quale il datore di lavoro deve adottare le misure che secondo la



particolarità del lavoro, l'esperienza e la tecnica sono necessarie per tutelare l'integrità fisica e morale dei lavoratori.

Va infine tenuto presente che la giurisprudenza ritiene che i reati in questione siano imputabili al datore di lavoro anche qualora la persona offesa non sia un lavoratore, ma un estraneo, purché la sua presenza sul luogo di lavoro al momento dell'infortunio non abbia caratteri di anormalità ed eccezionalità.

D.2. Individuazione delle attività sensibili

Tenuto conto dell'organizzazione e dell'attività del Comitato Regionale, costituiscono attività sensibili ai sensi del Decreto le seguenti attività:

- ✓ Omologare i campi di calcio (ivi inclusi quelli di calcio femminile e calcio a 5) di sua competenza in conformità alle norme federali vigenti;
- ✓ Nominare il Responsabile del Servizio di Prevenzione e Protezione per gestire e coordinare le attività di prevenzione e protezione dai rischi professionali per i lavoratori sensi del d.lgs. 81/2008 e successive modifiche ed integrazioni;
- ✓ Utilizzare collaboratori/volontari per supportare le attività dei propri dipendenti sia presso la sede sia presso le delegazioni provinciali;
- ✓ Intrattenere rapporti con la L.N.D. per la gestione del Personale e la realizzazione e gestione dei sistemi informativi.

D.3. Individuazione delle funzioni coinvolte

Tenuto conto dell'operatività del Comitato Regionale, gli uffici ed i soggetti apicali ritenuti più specificamente a rischio sono:

- ✓ Presidente;
- ✓ Consiglio Direttivo;
- ✓ Segretario;
- ✓ Fiduciario Campi Sportivi;



- ✓ Ufficio Omologazione Campi.
- ✓ RSPP.

D.4. Presidi organizzativi

I presidi organizzativi/controlli *specifici* posti in essere dal Comitato Regionale Campania, in relazione alle sopra indicate attività sensibili, che possono essere considerati a prevenzione dei reati di omicidio colposo e lesioni personali gravi, prevedono che:

- ✓ Sia nominato un Responsabile del Servizio Protezione e Prevenzione - RSPP, ai sensi del d.lgs. 81/2008, garantendo che lo stesso possieda le capacità e i requisiti professionali previsti dall'art. 32 dello stesso d.lgs.;
- ✓ Siano attribuiti al Responsabile Servizio Protezione e Prevenzione specifici poteri per fare fronte alla nomina ricevuta, ottenendo accettazione della stessa;
- ✓ Il Responsabile Servizio Protezione e Prevenzione adempia a tutti i compiti a lui affidati, vigilando sull'osservanza delle disposizioni di sicurezza in sede;
- ✓ Il Presidente, con il supporto del Segretario, verifichi l'adempimento degli obblighi delegati a dirigenti e preposti in materia di sicurezza;
- ✓ Qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia di salute e sicurezza sul lavoro, i contratti con tali soggetti debbano contenere apposita dichiarazione di conoscenza della normativa di cui al d.lgs. n. 231/2001 e di impegno al suo rispetto;
- ✓ Non siano affidati incarichi ad eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su professionalità qualificata, competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta siano ispirate ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dal R.A.C. della L.N.D.;



- ✓ Sia adottata una condotta trasparente e collaborativa nei confronti degli enti preposti al controllo (es. Ispettorato del Lavoro, ASL, Vigili del Fuoco, etc.) in occasione di accertamenti/procedimenti ispettivi;
- ✓ A tutti i collaboratori e volontari sia consegnato un *vedemecum* relativo alle norme di sicurezza inerenti i comportamenti e le precauzioni da osservare presso gli uffici del Comitato. Sia firmata da ciascun collaboratore e volontario una specifica dichiarazione di avvenuta ricezione del documento e di impegno al rispetto delle disposizioni contenute al suo interno.
- ✓ L'omologazione dei campi sia effettuata secondo le linee guida emanate dalla L.N.D. e svolta da professionisti qualificati. A supporto dell'omologazione sia redatto un apposito verbale a firma del Fiduciario Campi Sportivi e ad esso siano allegare delle foto dei luoghi ispezionati.

I presidi organizzativi *generici* che devono essere posti in essere dal Comitato (Codici, Misure organizzative, Sistemi informatici, Procedure), a fronte dei reati di omicidio colposo e lesioni personali gravi, sono i seguenti:

- ✓ Attenta verifica ed eventuale integrazione delle procedure interne di prevenzione ai sensi dei principi ex d.lgs. n. 231/2001 in coerenza con la specificità dei rischi di violazione delle norme richiamate dall'art. 25-septies del d.lgs. n. 231/2001; a tal fine è importante tenere conto di tutte le attività già svolte, anche in materia di gestione della sicurezza, armonizzandole anche ai fini dell'allineamento a quanto previsto dal d.lgs. n. 231/2001, evitando inutili quanto costose duplicazioni;
- ✓ Valutazione ed individuazione dei raccordi tra i vari soggetti coinvolti nel sistema di controllo ai sensi del d.lgs. n. 231/2001 e delle normative speciali in materia di sicurezza e salute sui luoghi di lavoro, con particolare riferimento alla previsione di un sistema integrato di controllo riguardante il RSPP, o altro soggetto giuridicamente equivalente, qualificabile come controllo tecnico-operativo di primo grado, e l'OdV incaricato del controllo sulla efficienza ed efficacia delle procedure rilevanti ai sensi del d.lgs. n. 231/2001, o controllo di secondo grado;



- ✓ Promozione dell'informazione e della formazione interna in tema di rischi connessi allo svolgimento delle attività, misure ed attività di prevenzione e protezione adottate, procedure di pronto soccorso, lotta antincendio ed evacuazione dei lavoratori;
- ✓ Pieno rispetto delle normative in tema di salute e sicurezza nei confronti di tutti i lavoratori non dipendenti, con particolare riferimento all'ambito dei contratti regolati dal d.lgs. 10 settembre 2003 n. 276 e successive modifiche ed integrazioni, nonché nei confronti dei soggetti beneficiari di iniziative di tirocinio e dei terzi in genere che dovessero trovarsi nei luoghi di lavoro.



E. DELITTI INFORMATICI

La presente “Parte Speciale” del Modello si riferisce ai reati informatici ed al trattamento illecito dei dati. Si descrivono brevemente qui di seguito le fattispecie contemplate dal Decreto, che potrebbero trovare eventualmente manifestazione all’interno del Comitato Regionale.

E.1 Ipotesi di Reato

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

Il reato è commesso da chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo. Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema; può pertanto realizzarsi anche qualora lo scopo sia di dimostrare la propria abilità e la vulnerabilità dei sistemi altrui, anche se più frequentemente l’accesso abusivo avviene al fine di danneggiamento o è propedeutico alla commissione di frodi o di altri reati informatici. Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali: verificarsi della distruzione o del danneggiamento dei dati, dei programmi o del sistema, o dell’interruzione totale o parziale del suo funzionamento; o quando si tratti di sistemi di interesse pubblico o di fatti compiuti con abuso della qualità di operatore del sistema. Nel contesto organizzativo il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, a banche dati del Comitato, mediante l’utilizzo delle credenziali di altri colleghi abilitati.

Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)

L’art. 615-*quater* c.p. punisce chiunque al fine di procurare a sé od ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o



consegna codici, parole chiave o altri mezzi idonei all'accesso di un sistema protetto da misure di sicurezza o comunque fornisce indicazioni idonee al predetto scopo. L'art. 615-*quinquies* c.p. punisce chiunque si procura, produce, riproduce, importa, diffonde, comunica, consegna o mette a disposizione di altri apparecchiature, dispositivi o programmi allo scopo di danneggiare illecitamente un sistema od i dati ed i programmi ad esso pertinenti ovvero di favorire l'interruzione o l'alterazione del suo funzionamento. Tali fattispecie perseguibili d'ufficio, intendono reprimere anche la sola abusiva detenzione o diffusione di credenziali di accesso o di programmi (virus, *spyware*) o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli altri crimini informatici sopra illustrati, rispetto ai quali le condotte in parola possono risultare propedeutiche. La prima fattispecie richiede che il reo agisca a scopo di lucro o di altrui danno. Peraltro, nella valutazione di tali condotte potrebbe assumere preminente rilevanza la considerazione del carattere obiettivamente abusivo di trasmissioni di dati, programmi, e-mail, etc., da parte di chi, pur non essendo mosso da specifica finalità di lucro o di causazione di danno, sia a conoscenza della presenza in essi di virus che potrebbero determinare gli eventi dannosi descritti dalla norma.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.) Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)

La condotta punita dall'art. 617-*quater* del codice penale consiste nell'intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, o nell'impedimento od interruzione delle stesse. Integra la medesima fattispecie, salvo che il fatto non costituisca un più grave reato, anche la diffusione mediante qualsiasi mezzo di informazione al pubblico del contenuto delle predette comunicazioni. L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di *software* (c.d. *spyware*). L'impedimento od interruzione delle comunicazioni (c.d. "*Denial of service*") può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impiego di virus informatici, ma anche ad esempio sovraccaricando il sistema con l'immissione di numerosissime



comunicazioni fasulle. Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali rientrano le condotte commesse in danno di un sistema utilizzato dallo Stato o da altro ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità o con abuso della qualità di operatore di sistema. Nell'ambito aziendale l'impedimento o l'interruzione potrebbero essere ad esempio causati dall'installazione non autorizzata di un *software* da parte di un dipendente. L'art. 617-*quinquies* c.p. punisce il solo fatto dell'installazione, fuori dai casi consentiti dalla legge, di apparecchiature atte ad intercettare, impedire od interrompere le comunicazioni, indipendentemente dal verificarsi di tali eventi. Il delitto è perseguibile d'ufficio.

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

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)

L'art. 635-*bis* c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime informazioni, dati o programmi informatici altrui. L'art. 635-*ter* c.p., salvo che il fatto costituisca più grave reato, punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti dall'articolo che precede, a prescindere dal prodursi in concreto del risultato del danneggiamento, che se si verifica costituisce circostanza aggravante della pena. Deve però trattarsi di condotte dirette a colpire informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Rientrano pertanto in tale fattispecie anche le condotte riguardanti dati, informazioni e programmi utilizzati da enti privati, purché siano destinati a soddisfare un interesse di pubblica necessità. Entrambe le fattispecie sono aggravate se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. Il primo reato è perseguibile a querela della persona offesa o d'ufficio, se ricorre una delle circostanze aggravanti previste; il secondo reato è sempre perseguibile d'ufficio. Qualora le condotte descritte conseguano ad un accesso abusivo al sistema esse saranno punite ai sensi del sopra illustrato art. 615-*ter* c.p.



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

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

L'art. 635-*quater* c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-*bis*, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto od in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. Per dirsi consumato il reato in oggetto, il sistema su cui si è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve essere ostacolato il funzionamento. L'art. 635-*quinquies* c.p. punisce le medesime condotte descritte nell'articolo che precede anche se gli eventi lesivi non si realizzino in concreto; il loro verificarsi costituisce circostanza aggravante della pena (va però osservato che il concreto ostacolo al funzionamento del sistema non rientra espressamente fra gli "eventi" aggravanti). Deve però trattarsi di condotte che mettono in pericolo sistemi informatici o telematici di pubblica utilità. In questa previsione, a differenza di quanto previsto all'art. 635-*ter*, non vi è più alcun riferimento all'utilizzo da parte di enti pubblici: per la configurazione del reato in oggetto, parrebbe quindi che i sistemi aggrediti debbano essere semplicemente "di pubblica utilità"; non sarebbe cioè, da un lato, sufficiente l'utilizzo da parte di enti pubblici e sarebbe, per altro verso, ipotizzabile che la norma possa applicarsi anche al caso di sistemi utilizzati da privati per finalità di pubblica utilità. Entrambe le fattispecie sono perseguibili d'ufficio e prevedono aggravanti di pena se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. E' da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di dati e programmi qualora queste rendano inutilizzabili i sistemi o ne ostacolino gravemente il regolare funzionamento. Qualora le condotte descritte conseguano ad un accesso abusivo al sistema, esse saranno punite ai sensi del sopra illustrato art. 615-*ter* c.p.

Falsità nei documenti informatici (art. 491 bis c.p.)

L'art. 491-*bis* c.p. dispone che ai documenti informatici pubblici o privati aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con



riguardo ai tradizionali documenti cartacei, previste e punite dagli artt. da 476 a 493 c.p. Il concetto di documento informatico è nell'attuale legislazione svincolato dal relativo supporto materiale che lo contiene, in quanto l'elemento penalmente determinante ai fini dell'individuazione del documento informatico consiste nell'attribuibilità allo stesso di un'efficacia probatoria secondo le norme civilistiche. Nei reati di falsità in atti è fondamentale la distinzione tra le falsità materiali e le falsità ideologiche: ricorre la falsità materiale quando vi sia divergenza tra l'autore apparente e l'autore reale del documento o quando questo sia stato alterato (anche da parte dell'autore originario) successivamente alla sua formazione; ricorre la falsità ideologica quando il documento contenga dichiarazioni non veritiere o non fedelmente riportate. Con riferimento ai documenti informatici aventi efficacia probatoria, il falso materiale potrebbe compiersi mediante l'utilizzo di firma elettronica altrui, mentre appare improbabile l'alterazione successiva alla formazione. Non sembrano poter trovare applicazione, con riferimento ai documenti informatici, le norme che puniscono le falsità in fogli firmati in bianco (artt. 486, 487 e 488 c.p.).

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

Tale reato è commesso dal soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. Il soggetto attivo del reato può essere evidentemente soltanto un soggetto "certificatore qualificato", che esercita particolari funzioni di certificazione per la firma elettronica qualificata.

E.2. Individuazione delle attività sensibili

Tenuto conto dell'organizzazione e dell'attività del Comitato Regionale, costituiscono attività sensibili ai sensi del Decreto le seguenti attività:

- ✓ Gestire i sistemi informativi di propria competenza e l'aggiornamento del proprio sito internet;



- ✓ Intrattenere rapporti con le strutture centrali della L.N.D. per la gestione del Personale e la gestione dei sistemi informativi.

E.3. Individuazione delle funzioni coinvolte

Tenuto conto dell'operatività del Comitato Regionale, gli uffici ed i soggetti apicali ritenuti più specificamente a rischio sono:

- ✓ Presidente;
- ✓ Segretario;
- ✓ Responsabile Amministrativo;
- ✓ Ufficio Amministrazione.

E.4. Presidi organizzativi

I presidi organizzativi/controlli *specifici* posti in essere dal Comitato Regionale, in relazione alle sopra indicate attività sensibili, che possono essere considerati a prevenzione dei reati informatici, prevedono che:

- ✓ La Sicurezza informatica sia garantita:
 - ✓ a livello di rete da un sistema passivo di difesa perimetrale (*firewall*) che filtra il traffico in svolgimento da/verso l'esterno della rete ed un sistema attivo che identifica la natura dei pacchetti in transito eliminando quelli appartenenti ad applicazioni il cui utilizzo non è consentito (P2P, streaming audio e video, etc.).
 - ✓ a livello *server/client* da specifici prodotti antivirus.
- ✓ I dati e le informazioni non pubbliche, relative anche alle società sportive e terze parti (commerciali e tecniche), incluse le modalità di connessione da remoto, devono essere gestite come riservate;
- ✓ A tutti i dipendenti, consulenti e collaboratori/volontari del Comitato sia vietato:



- introdurre nel Comitato computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del soggetto responsabile individuato;
- modificare la configurazione di postazioni di lavoro fisse o mobili;
- acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.);
- ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dal Comitato o dalla L.N.D.;
- divulgare, cedere o condividere con personale interno o esterno al Comitato Regionale le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- accedere senza autorizzazione ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici del Comitato Regionale o di società terze, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- comunicare a persone non autorizzate, interne o esterne al Comitato Regionale, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati sia all'interno del singolo Comitato Regionale Campania sia all'interno della L.N.D.;



- distorcere, oscurare, sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati.

I presidi organizzativi *generici* che devono essere posti in essere dal Comitato Regionale (Codici, Misure organizzative, Sistemi informatici, Procedure), a fronte dei reati informatici, sono i seguenti:

- ✓ Sistema di controlli interno alla Comitato Regionale che preveda ai fini del corretto e legittimo accesso (eventuale) ai Sistemi informativi della Pubblica Amministrazione:
 - un adeguato riscontro delle password di abilitazione per l'accesso ai sistemi informativi della P.A. possedute, per ragioni di servizio, da determinati Dipendenti appartenenti a specifiche funzioni/strutture organizzative;
 - la puntuale verifica dell'osservanza, da parte dei Dipendenti medesimi, di ulteriori misure di sicurezza adottate dal Comitato Regionale e/o dalla L.N.D.;
 - il rispetto della normativa sulla privacy a tutela del Dipendente.
- ✓ Adeguata informazione a tutti i Dipendenti su l'importanza di mantenere i propri codici di accesso (username e password) confidenziali e di non divulgare gli stessi a soggetti terzi;
- ✓ Sottoscrizione da parte dei Dipendenti e agli altri soggetti eventualmente autorizzati di uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche del Comitato;
- ✓ Sensibilizzazione dei Dipendenti e degli altri soggetti eventualmente autorizzati sulla necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;



- ✓ Non permettere l'utilizzo dei sistemi informatici del Comitato Regionale Campania da parte dei Dipendenti per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico della L.N.D.
- ✓ Tutti i dipendenti, consulenti, collaboratori e volontari del Comitato sono tenuti a conoscere ed osservare tutte le regole e i principi contenute nella politica della L.N.D. relativa alla gestione degli accessi logici a reti, sistemi, dati e applicazioni (D.P.S.) e relativa alla gestione delle credenziali personali (*username* e *password*).



F. REATI CONTRO LA PERSONALITA' INDIVIDUALE

La presente “Parte Speciale” del Modello si riferisce ai reati contro la personalità individuale. Si descrivono brevemente qui di seguito le fattispecie contemplate dal Decreto, che potrebbero trovare eventualmente manifestazione all’interno del Comitato Regionale Campania.

F.1. Ipotesi di reato

Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.); Prostituzione minorile (art. 600-bis c.p.); Pornografia minorile (art. 600-ter c.p.); Detenzione di materiale pornografico (art. 600-quater); Tratta di persone (art. 601 c.p.); Acquisto e alienazione di schiavi (art. 602 c.p.); Pornografia virtuale (art. 600-quater.1 c.p.); Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.)

Per alcuni dei reati sopra richiamati è difficile individuare la sussistenza di un interesse o vantaggio per il Comitato Regionale (es. prostituzione minorile) ma per tale motivo è importante sottolineare che tali ipotesi di reato si estendono non solo al soggetto che direttamente realizza la fattispecie illecita, ma anche a chi consapevolmente agevola anche solo finanziariamente la medesima condotta.

In quest’ottica il Comitato Regionale, al fine di prevenire i rischi legati a tale tipologia di reati, può intraprendere anche visite ispettive presso i propri fornitori ovvero richiedere ai fornitori medesimi ogni documentazione utile.

F.2. Individuazione delle attività sensibili

Tenuto conto dell’organizzazione e dell’attività del Comitato Regionale Campania, costituiscono attività sensibili ai sensi del Decreto le seguenti attività:

- ✓ Assumere impegni di spesa nell'ambito delle previsioni del P.E.P.O. e nelle modalità e limiti previsti dal R.A.C.



F.3. Individuazione delle funzioni coinvolte

Tenuto conto dell'operatività del Comitato Regionale, gli uffici ed i soggetti apicali ritenuti più specificamente a rischio sono:

- ✓ Presidente;
- ✓ Consiglio Direttivo;
- ✓ Consiglio di Presidenza;
- ✓ Segretario.

F.4. Presidi organizzativi

I presidi organizzativi/controlli *specifici* posti in essere dal Comitato Regionale Campania, in relazione alle sopra indicate attività sensibili, che possono essere considerati a prevenzione dei reati contro la personalità individuale ed in particolare dei reati di riduzione o mantenimento in schiavitù o in servitù, prevedono che:

- ✓ Vi sia un controllo accurato delle proposte di fornitura avendo cura in primo luogo degli aspetti regolamentari - normativi e di sicurezza piuttosto che alle condizioni economiche applicate.
- ✓ L'attività di ricerca dei fornitori sia svolta nel rispetto del R.A.C. e del Codice Etico adottato dalla L.N.D. La scelta del fornitore, inoltre, per gli acquisti di beni o servizi di valore rilevante, dovrà essere effettuata avendo riguardo all'apposito Albo Fornitori del Comitato Regionale.

I presidi organizzativi *generici* che devono essere posti in essere dal Comitato Regionale (Codici, Misure organizzative, Sistemi informatici, Procedure), a fronte dei reati contro la personalità individuale ed in particolare dei reati di riduzione o mantenimento in schiavitù o in servitù, sono i seguenti:

- ✓ Prevedere, nel Codice Etico, uno specifico impegno a rispettare ed a far rispettare ai propri fornitori la normativa vigente in materia di lavoro, con particolare



attenzione al lavoro minorile ed a quanto disposto dalla legge in tema di salute e sicurezza;

- ✓ Richiedere e verificare che i propri partner rispettino gli obblighi di legge in tema di:
 - tutela del lavoro minorile e delle donne;
 - condizioni igienico-sanitarie e di sicurezza;
 - diritti sindacali o comunque di associazione e rappresentanza.